Chapter 7

Finite groups

Introduction

In Chapter 6 we classified cyclic groups, and abelian groups whose order is a product of distinct prime numbers. In this chapter we explore certain more general classes of finite groups, not necessarily abelian, including all groups of order up to 14.

We start by finding a method of writing group elements so that we can manipulate them in a way that generalises what we do for cyclic groups, where we can write every element as a power of a generator. In this way, we can work with larger finite groups for which writing down a Cayley table would be impractical. In the process, we introduce a new class of groups known as *dicyclic* groups.

We move on to link group actions to conjugacy and introduce the idea of the *centre* of a group G, that is, the set of all those elements that commute with every other element of G. We apply the tools at our disposal to classify groups of order p^2 and groups of order $2p$ where p is an odd prime. These results cover groups of order 4, 9, 6, 10 and 14. We then give ad hoc results for groups of order 8 and 12. In this way, and using our knowledge of the structure of groups of prime order, we obtain a classification of finite groups of order up to 14.

In the final section we explore the structure of finite groups whose order is a power of a prime p, known as *finite p-groups*.

Chapter guide

In terms of study time, Section 1 should be similar to Section 2. Section 2 builds on notions that you will begin to find familiar by now.

Section 3 is fairly theoretical: some of the proofs are quite technical, but they are particularly interesting because they make use of many results and notions from previous chapters. There are few exercises, mainly intended to provide some of the steps in the various proofs.

Section 4 is slightly shorter, with one important theorem and proof, and few exercises.

1 Describing groups

The idea that a single group element *generates* a (cyclic) subgroup by repeated applications of the group operation can be generalised to the case of a finite set of elements. This section introduces the notion of a set of generators of a group and a set of *relations* among the generators. As an example, it looks at a family of finite groups called the dicyclic groups, describing them in terms of generators and relations.

1.1 Generators and relations

A group with 12 elements, such as D_6, the symmetry group of the regular hexagon, is really too large to deal with conveniently by a Cayley table. In this section we formally introduce a way of describing a group using generators. We have been using this approach informally in the previous two chapters, and in this section we will take a more rigorous approach.

Our aim is to find a more succinct way of describing the elements of D_6 than by simply listing all 12 elements. In Chapter 6, we used this approach when working with the action of D_6 on itself by conjugation. We would like this description to aid us with manipulating elements in the same way that in $\mathbb{Z}_7$ (say) we can write any element as a power of a generator a, and can write the composition of two elements a^2 and a^3 (say) as $a^2a^3 = a^5$.

The term 'generators' is an extension of the term 'generator' that you met in the context of cyclic groups. We will start this section by describing D_6 in this way. In the following discussion, you can think of the generators as being the elements involved in our succinct description and of the relations as being the rules we need to carry out manipulations.

It is fairly easy to spot a possible generator for all the rotations: for example, the rotation anticlockwise about the centre through $\frac{\pi}{3}$ can be used to produce all the rotations (including the identity).

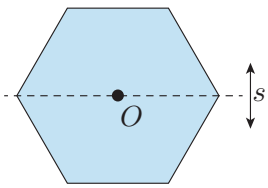


Figure 1.1 Reflection of a hexagon in a given line

Composing rotations with the same centre always produces a rotation and never a reflection. As a consequence, a set of generators of D_6 must contain a reflection, since the whole group does. Consider, for example, the reflection in the line shown in Figure 1.1.

Let us label the chosen rotation r and the chosen reflection s. In the following exercise, you are asked to show that these two elements generate D_6. In fact, as you may wish to check, the reflection s is not the only possible choice: *any* reflection will do.

In the notation of M208, $r = r_{\pi/3}$ and $s = q_0$. We have chosen shorter labels for convenience in the calculations that follow.

Exercise 1.1

Let s be the reflection of the hexagon shown in Figure 1.1, and let r be the anticlockwise rotation through $\frac{\pi}{3}$ about the centre of the hexagon.

(a) Express each of the six rotations in D_6 as powers of r.

(b) Express each of the six reflections in D_6 in the form $r^n s$, for suitable integers n.

(c) Since sr must be a group element (by the closure axiom), it must be one of the elements found in the solutions to parts (a) and (b). Which one?

The solution to Exercise 1.1 gives a description of D_6 that will make calculations with its elements much easier. The group D_6 is generated by two elements r and s about which we know the following:

$$r^6 = s^2 = e, \quad sr = r^5 s.$$

Note that the second equation can also be written

$$sr = r^{-1}s.$$

We use these equations to describe the group as follows:

$$D_6 = \langle r, s \,|\, r^6 = s^2 = e,\ sr = r^5 s \rangle.$$

In this description of D_6, the elements r and s are known as the *generators* of the group, and the equations $r^6 = s^2 = e,\ sr = r^5 s$ as the *relations*. We have further information about D_6, namely that every element can be written uniquely in the form

$$r^i s^j \quad \text{for } i = 0, \ldots, 5 \quad \text{and} \quad j = 0, 1.$$

Note that, since $r^0 = s^0 = e$, we usually write $r^i s^0$ as r^i and $r^0 s^j$ as s^j. Thus, elements of D_6 have a **standard form**. The existence of such a standard form enables computations to be made without recourse to a Cayley table.

In practice if, for a given group G, we know

- two generators a and b
- the orders of the two generators
- a relation indicating how to write ba as $a^m b^n$ for some m, n

For an abelian group, for example, we have the relation $ba = ab$.

then we have enough information to write the elements of G in a standard form $a^i b^j$.

This means that we can give an alternative complete and compact description of D_6 as follows:

$$D_6 = \{r^i s^j : i = 0, \ldots, 5,\ j = 0, 1;\ r^6 = s^2 = e,\ sr = r^5 s\}.$$

Note that we have used set notation here, rather than angled brackets. This is because you can read this description of D_6 as 'the set of expressions of the form $r^i s^j$ where $i = 0, \ldots, 5,\ j = 0, 1;\ r^6 = s^2 = e$ and $sr = r^5 s$'.

The information on the orders of the generators and the relation between them can be used to express any element of D_6 in standard form. As an example, here is how to find the standard form of the product $sr^2 s$.

$$\begin{aligned} sr^2 s &= srrs \\ &= r^5 srs && \text{using } sr = r^5 s \\ &= r^5 r^5 ss && \text{using } sr = r^5 s \text{ again} \\ &= r^{10} e && \text{using } s^2 = e \\ &= r^4 && \text{using } r^6 = e \end{aligned}$$

Exercise 1.2

Let $D_6 = \{r^i s^j : i = 0, \ldots, 5,\ j = 0, 1;\ r^6 = s^2 = e,\ sr = r^5 s\}$.

(a) Use the relations given to express sr^2 and sr^3 in standard form.

(b) Write s^5 in standard form.

The description $D_6 = \langle r, s \mid r^6 = s^2 = e,\ sr = r^5 s\rangle$ is known as a **group presentation**. In general, a group presentation consists of a set of **generators** $g_1, g_2, \ldots, g_n$, say, and a set of equations known as **relations**. Sometimes the relations are given as expressions involving the generators that equate to the identity. Such presentations assume the existence of inverses of the generators as well as the existence of the identity e. It is possible to formally define a group presentation and to define the group described by any such presentation, but we will not do this here. We will just note the properties we need as follows.

Properties of a group presentation

Let G be a group with presentation

$$G = \langle g_1, g_2, \ldots, g_n \mid r_1, r_2, \ldots, r_m\rangle.$$

1. Any element of the group can be written in the form

   $$g_{i_1}^{n_1} g_{i_2}^{n_2} \cdots g_{i_s}^{n_s},$$

   where $i_1, \ldots, i_s \in \{1, 2, \ldots, n\}$ and $n_i \in \mathbb{Z}$. In this expression there may be repetitions of a generator, and the powers can be both positive and negative.
2. Any equation that holds in the group can be derived from the given relations.

Expressions such as $g_{i_1}^{n_1} g_{i_2}^{n_2} \cdots g_{i_s}^{n_s}$ are known as **words**.

There is a famous issue with this form of presentation, known as the *word problem*, whereby it is not always possible to know whether two words w_1 and w_2 are equal. In other words, it is not always possible to know whether the equality $w_1 = w_2$ can be derived from the given relations. Luckily, the word problem does not arise in the groups we discuss in this module.

For some groups, such as the dihedral groups, elements have a standard form.

Definition 1.1 *Standard form of elements*

Let G be a group with presentation

$$G = \langle g_1, g_2, \ldots, g_n \mid r_1, r_2, \ldots, r_m \rangle.$$

Then we say that elements of G have a **standard form** if every element of G can be written uniquely as a product of powers of the generators according to a specified pattern.

When it is possible to find a standard form for the elements of a certain group, it is also possible to give an alternative presentation of the group whereby the list of generators is replaced by the standard form of the elements of the group. We have done this above for D_6, where we have used the presentation

$$D_6 = \{r^i s^j : \ i = 0, \ldots, 5, \ j = 0, 1; \ r^6 = s^2 = e, \ sr = r^5 s\},$$

where, as remarked earlier, we use set notation rather than angled brackets.

Exercise 1.3

By what names do you know the groups with the following presentations?

(a) $\{r^i : i = 0, \ldots, 5; \ r^6 = e\}$

(b) $\{r^i s^j : i = 0, \ldots, 3, \ j = 0, 1; \ r^4 = s^2 = e, \ sr = r^3 s\}$

(c) $\{r^i s^j : i = 0, 1, \ j = 0, 1; \ r^2 = s^2 = e, \ sr = rs\}$

Recall from Section 1 of Chapter 5 that there is a whole family of dihedral groups, one for each regular polygon. The **dihedral group** D_n is the symmetry group of the regular n-gon, and it has order $2n$. As you can probably see, all dihedral groups can be described in the following way:

$$D_n = \{r^i s^j : i = 0, \ldots, n-1, \ j = 0, 1; \ r^n = s^2 = e, \ sr = r^{n-1} s\}.$$

The next exercise and example are designed to give you practice in working with this type of group presentation. You are asked to work with the dihedral group D_4. Before you start, it is worth convincing yourself that the elements of D_4 may be generated by a rotation r through $\frac{\pi}{2}$ about the centre of the square and a reflection s in an axis through the centre of the square and parallel to two of its sides.

Exercise 1.4

Let G be the group of symmetries of the square, denoted by D_4. In other words,

$$G = \{r^i s^j : i = 0, 1, 2, 3,\ j = 0, 1;\ r^4 = s^2 = e,\ sr = r^3 s\}$$
$$= \{e, r, r^2, r^3, s, rs, r^2 s, r^3 s\}.$$

Let N be the set $\{e, r^2\}$.

(a) Prove that N is a normal subgroup of G.

(b) Find the set of left cosets of N in G in the form aN where $a \in G$.

(c) Using your notation in part (b), write out the Cayley table of the quotient group G/N.

Example 1.2 *D_6 and the Correspondence Theorem*

Let $D_6 = \langle r, s \mid r^6 = s^2 = e, sr = r^5 s = r^{-1} s \rangle$ and let $N = \{e, r^3\}$.

It is not difficult to check that r^3 commutes with every other element of D_6 and that $(r^3)^2 = e$, so N is a normal subgroup of D_6. This implies that the quotient D_6/N is a group, whose elements are

$$\begin{array}{lll} N & = \{e, r^3\} & = r^3 N, \\ rN & = \{r, r^4\} & = r^4 N, \\ r^2 N & = \{r^2, r^5\} & = r^5 N, \\ sN & = \{s, r^3 s\} & = r^3 sN, \\ rsN & = \{rs, r^4 s\} & = r^4 sN, \\ r^2 sN & = \{r^2 s, r^5 s\} & = r^5 sN. \end{array}$$

So $D_6/N = \{N, rN, r^2 N, sN, rsN, r^2 sN\} \cong D_3$. We now apply the Correspondence Theorem to D_6/N to understand the structure of D_6.

You can check that in this copy of D_3, the identity is N, the two non-trivial rotations are rN and $r^2 N$, and sN, rsN, $r^2 sN$ are the three reflections.

Now consider the subgroup $H = \{e, r, r^2, r^3, r^4, r^5\}$ of D_6. This subgroup contains N, and it is a normal subgroup of index 2 in D_6.

Thus, by the Correspondence Theorem, H/N is a normal subgroup of D_6/N of index 2 in D_6/N. Since $H/N = \{hN :\ h \in H\}$, the elements of H/N are as follows.

$$\begin{array}{ll} N & = \{e, r^3\} \\ rN & = \{r, r^4\} \\ r^2 N & = \{r^2, r^5\} \end{array}$$

So $H/N = \{N, rN, r^2 N\}$, which is indeed a normal subgroup of D_6/N of index 2: it corresponds to the subgroup of three rotations in D_3 (remember that the identity is a rotation through 0).

Now, the group D_3 has three non-normal subgroups of order 2 and index 3, each of which contains the identity and a reflection.

As a subgroup of D_6/N, one of these three non-normal subgroups is

$$\overline{K} = \{N, sN\}.$$

Since $(sN)^2 = s^2N = eN = N$, we know that sN is self-inverse.

By the Correspondence Theorem, D_6 has a non-normal subgroup K of index 3 that contains N and for which $K/N = \{N, sN\} = \overline{K}$. Thus K is the union of two cosets of N, namely

$$K = N \cup sN = \{e, r^3\} \cup \{s, r^3 s\} = \{e, r^3, s, r^3 s\}.$$

Confirm this by finding K/N for $K = \{e, r^3, s, r^3 s\} \subseteq D_6$.

Finally, note the following.

- K is a subgroup containing N – in fact K is isomorphic to the Klein group, or D_2.
- $|K| = 4$ so the index of K in D_6 is $|D_6|/4 = 12/4 = 3$.
- $rK = \{r, r^4, rs, r^4 s\}$ whereas $Kr = \{r, r^4, r^5 s, r^2 s\} \neq rK$, so K is not normal in D_6.

Exercise 1.5

In the notation of Example 1.2, let $\overline{K}_1$ and $\overline{K}_2$ be the two non-normal subgroups of D_6/N not equal to K.

(a) Write down the elements of $\overline{K}_1$ and $\overline{K}_2$.

(b) Find the subgroups of D_6 that contain N which correspond to $\overline{K}_1$ and $\overline{K}_2$ as in the Correspondence Theorem.

Our findings about the Correspondence Theorem for D_6 in Example 1.2 and Exercise 1.5 are illustrated in Figure 1.2.

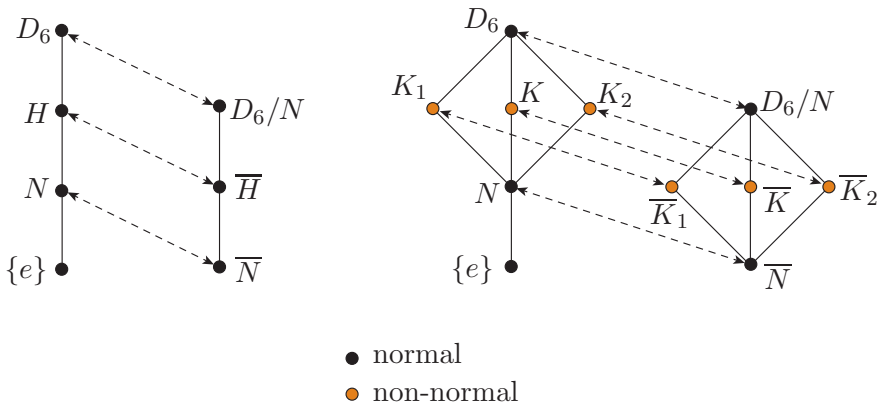


Figure 1.2 D_6 and the Correspondence Theorem

1.2 Dicyclic groups

Consider the group Dic_2 with presentation

$$\mathrm{Dic}_2 = \langle a, b \mid a^4 = e, a^2 = b^2, aba^3b = e \rangle.$$

This is the first in an important family of finite groups whose properties we will explore in this subsection.

Our first task will be to derive some properties of Dic_2 that follow from the relations $a^4 = e$, $a^2 = b^2$ and $aba^3b = e$.

Exercise 1.6

Show that the following hold in the group Dic_2:

(a) $b^4 = e$

(b) b^2 commutes with both a and b

(c) $ba = a^3b$

(d) any element g of Dic_2 can be written in the form $g = a^r b^s : \ r = 0, \ldots, 3, \ s = 0, 1$.

You may suspect, rightly, that in Exercise 1.6(d) we have found a standard form for the elements of Dic_2. However, to be sure that we really have a standard form we need to show that each element of Dic_2 can be written as $a^r b^s$, for suitable r and s, in a *unique* way.

Note that the expression $a^r b^s$ gives eight elements as r ranges over $0, \ldots, 3$ and s over $0, 1$. Thus, if we can find a group of eight elements with the given presentation, we will know that the expression $a^r b^s$ gives a standard form for its elements. You should be aware that there is no general way of finding such a group.

Consider the diagram in Figure 1.3. You may find it helpful to think of it as a dance formation or as the spokes of two wheels. In Figure 1.4 below, regard a as the dance move where the dancers (or the spokes of the two wheels) rotate anticlockwise through $\frac{\pi}{2}$.

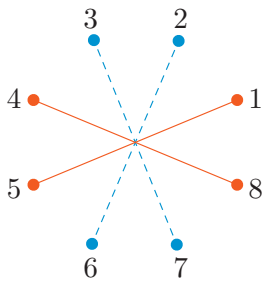


Figure 1.3 A dance formation

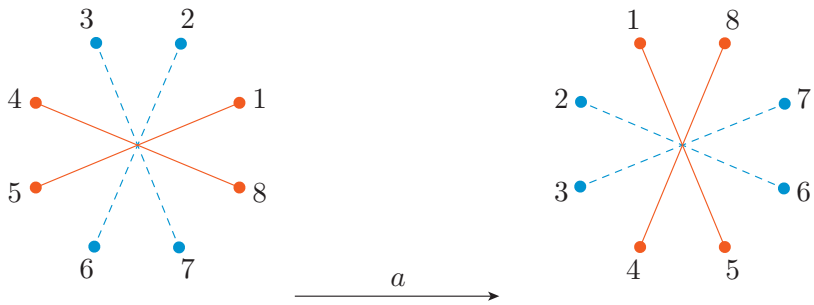


Figure 1.4 The effect of a on the dancers

Now regard b as the dance move where the two sets of dancers separate, rotate by one dancer in opposite directions and then come together again, or the move that rotates the two sets of spokes (one dashed and one solid) by one spoke but in opposite directions (Figure 1.5). The dancers (spokes) joined by solid lines move clockwise and the ones joined by a dotted line move anticlockwise.

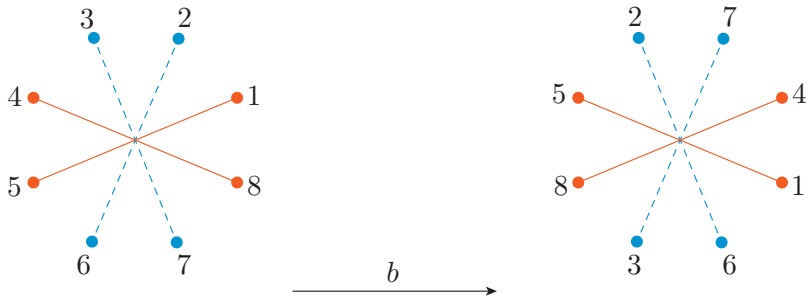


Figure 1.5 The effect of b on the dancers

If we regard a and b as permutations of the set of dancers (or spokes), these descriptions of a and b show that $a^4 = b^4 = e$. They also show that a followed by b is a permutation that reverses the direction of the dancers/spokes in b; that is, the solid lines now move anticlockwise and the dotted lines clockwise. This shows that $ba = ab^{-1} = ab^3$. Finally, you can observe that $a^2 = b^2$ (Figure 1.6).

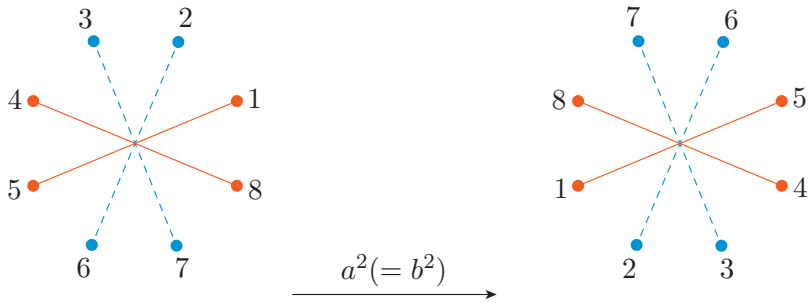


Figure 1.6 The effect of $a^2(= b^2)$ on the dancers

We have thus shown that a and b satisfy the relations in the presentation of the group Dic_2. Since the possible combinations of a and b give rise to eight different permutations of the dancers/spokes, we can see that these permutations form a group of order 8. This group is known as the **dicyclic** group of order 8. It is also known as the **quaternion group**.

In the next exercise you will see another characterisation of the group Dic_2 as a group of matrices over the complex numbers.

Recall that a **complex number** is an expression of the form

$$x + iy,$$

where x and y are real numbers and $i^2 = -1$. The set of all complex numbers is denoted by $\mathbb{C}$.

Exercise 1.7

(a) Let $\mathrm{GL}(2, \mathbb{C})$ be the group of invertible 2×2 matrices over the complex numbers, and let G be the subgroup of $\mathrm{GL}(2, \mathbb{C})$ whose generators are

$$a = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \quad \text{and} \quad b = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Show that $G \cong \mathrm{Dic}_2$.

(b) Show that G has three normal cyclic subgroups of order 4.

The quaternions are an extension of the complex numbers, and they were first described by the Irish mathematician Sir William Rowan Hamilton (1805–1865). A key fact about this extension is that it is a group where multiplication is not commutative. The quaternion group is the smallest multiplicative subgroup containing the three elements often known as i, j, k, where

$$i^2 = j^2 = k^2 = -1 \text{ and } ij = k, jk = i, ki = j.$$

The reason why Dic_2 has two names is that it is the smallest in a family of groups known as the *dicyclic groups*. The dance or wheel pictures help us to describe this family. Consider a dance formation with $4n$ dancers, or a pair of wheels with $4n$ spokes, $2n$ of which are dotted and $2n$ solid. The dancers, or spokes, are divided into four blocks with n dancers or spokes in each, arranged so that the dotted blocks are opposite one another and the solid blocks are opposite one another.

As before, we regard a as the dance move where the dancers, or spokes, rotate anticlockwise by $\frac{\pi}{2}$ (Figure 1.7).

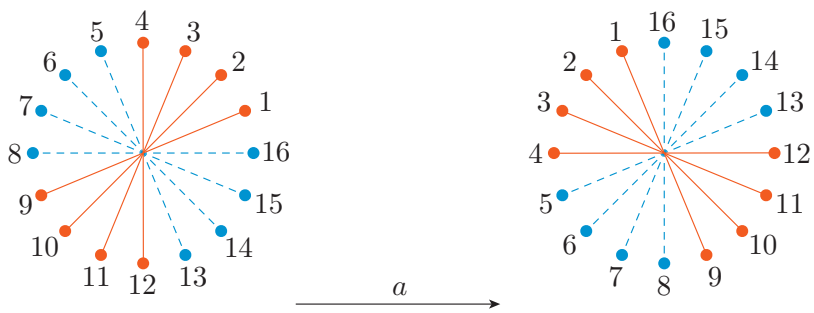


Figure 1.7 The effect of a on a formation of 16 dancers

Again, regard b as the dance move where the two sets of dancers separate, rotate by one dancer in opposite directions and then come together again, or the move that rotates the two sets of spokes (one dashed and one solid) by one spoke but in opposite directions (Figure 1.8). The dancers/spokes joined by solid lines move clockwise, and the ones joined by dotted lines move anticlockwise.

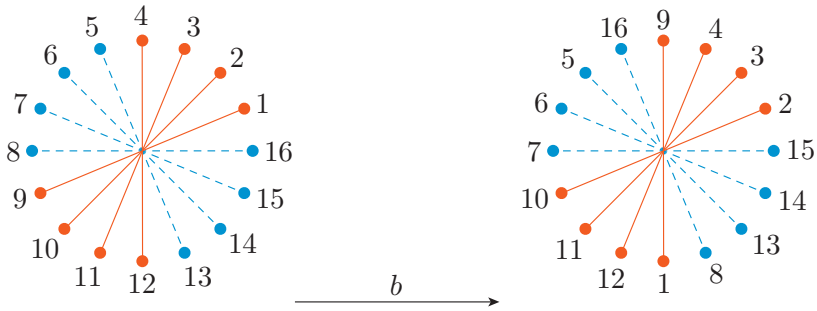


Figure 1.8 The effect of b on a formation of 16 dancers

We can see that in the general case of $4n$ dancers/spokes,

$$a^4 = e, \quad b^{2n} = e \quad \text{and} \quad a^2 = b^n.$$

Some thought may enable you to see that $ab = b^{-1}a$ or, equivalently, $aba^3b = e$. We can therefore give a presentation of the group described using $4n$ dancers/spokes as the **dicyclic group**

$$\mathrm{Dic}_n = \langle a, b \mid a^4 = e, a^2 = b^n, aba^3b = e \rangle.$$

Note that there are $4n$ possible positions of the dancers/spokes, so this group has order $4n$.

Adding dicyclic groups to our list of 'known' groups will enable us, by the end of this chapter, to describe all groups of order up to 14.

Exercise 1.8

Show that elements of Dic_n have a standard form given by

$$a^r b^s \quad \text{for } r = 0, \ldots, 3, \ s = 0, \ldots, n-1.$$

1.3 Describing subgroups using generators

We have used many times the idea of a subgroup *generated* by a particular element x of a group. Such a subgroup is a cyclic group denoted by $\langle x \rangle$, and its elements can be described precisely as follows:

$$\langle x \rangle = \{x^n : \ n \in \mathbb{Z}\}.$$

It is also possible to consider generating sets with more than one element, and in fact this is what we have done implicitly in Subsections 1.1 and 1.2

when working with generators in group presentations. For such generating sets, the situation becomes slightly more complex and much more interesting. Informally, we say that the subgroup of a group G generated by a set S is the smallest subgroup of G that contains S. By 'smallest', we mean a subgroup of G containing S that is contained in every other subgroup that contains S.

In what follows, we deal with the problem of whether such subgroups exist and what their elements look like.

Definition 1.3 *Subgroup generated by a set*

Let G be a group and S be a subset of (the underlying set of) G. We define the **subgroup H of G generated by S** to be a subgroup of G satisfying:

(a) $S \subseteq H$

(b) if K is a subgroup of G and $S \subseteq K$ then $H \subseteq K$.

We denote this subgroup by $\langle S \rangle$.

The notation $\langle S \rangle$ is a generalisation of the notation $\langle x \rangle$ used for cyclic subgroups generated by the single element x. To be consistent, we ought to change the previous notation to $\langle \{x\} \rangle$, though, like most mathematicians, we will not do so.

In the next lemma we prove the existence of subgroups generated by a set.

Lemma 1.4

Let G be a group and S be a subset of (the underlying set of) G. Then the group generated by S exists and is unique.

Proof To prove existence, consider the collection of all subgroups of G that contain the set S. This collection is certainly non-empty, since it contains the subgroup G.

Now, by Proposition 2.7 of Chapter 5, the intersection H of all of these subgroups is itself a subgroup of G. Furthermore, since each of the subgroups in the collection contains the set S, so does their intersection H. So H is a subgroup of G containing S.

In addition, if any subgroup of G contains the set S, it is in our collection and so it must contain the intersection H.

So H is a subgroup of G generated by S.

For uniqueness, suppose there is another subgroup J generated by S. Then $H \subseteq J$ and $J \subseteq H$ by condition (b) in Definition 1.3. Hence the two subgroups H and J are equal. This shows that the subgroup generated by S is unique. ■

Although Definition 1.3 and Lemma 1.4 cover infinite groups and infinite generating sets, in this module we will only be using them where the group is finite.

Worked Exercise 1.5

Consider the dicyclic group $\mathrm{Dic}_3 = \langle a, b \mid a^4 = e, a^2 = b^3, aba^3b = e\rangle$ and let $S = \{a^2, b^2\}$.

Find $H = \langle S\rangle$, the subgroup of Dic_3 generated by S.

Solution

Since Dic_3 has order 12, Lagrange's Theorem tells us that the group H must have order 2, 3, 4, 6 or 12.

Secondly, since a^2 has order 2, b^2 has order 3 and $a^2b^2 = b^2a^2$, we have that a^2b^2 has order 6 and so it generates a cyclic subgroup of order 6. We claim that $H = \langle a^2b^2\rangle$.

Now $\langle a^2b^2\rangle$ contains both $a^2 = (a^2b^2)^3$ and $b^2 = (a^2b^2)^4$. Thus H is contained in $\langle a^2b^2\rangle$.

But $\langle a^2b^2\rangle$ is contained in H, so $H = \langle a^2b^2\rangle$.

Since $a^2b^2 = b^5$, we have that H is in fact the cyclic group

$$\{e, b, b^2, b^3, b^4, b^5\}.$$

In standard form the elements of H are

$$\{e, b, b^2, a^2, a^2b, a^2b^2\}.$$

There is no systematic process to find the subgroup generated by a given subset of a group. The approach used in the previous exercise – that is, to find a subgroup containing the set and then show that this is the required subgroup – is typical of the arguments we can use.

Recall that the *alternating group* A_4 is the subgroup of S_4 consisting of the even permutations.

Exercise 1.9

Let $S = \{(1\,2\,3), (1\,2)(3\,4)\}$. Show that $\langle S\rangle = A_4$.

Before formally defining the subgroup generated by a subset S of a group G, we worked with the subgroup containing all products of powers of elements in S. The next proposition shows that this subgroup is in fact $\langle S\rangle$.

Lemma 1.6

Let G be a group and let S be a non-empty finite subset of G. Then the set

$$H = \{s_1^{r_1} \cdots s_n^{r_n} : n \in \mathbb{N},\ s_i \in S,\ r_i \in \mathbb{Z}, i = 1, \ldots, n\}$$

is a subgroup of G.

Proof We use the subgroup criterion, Proposition 2.4 of Chapter 5.

First, let $s \in S$. Then $e = s^0 \in H$ and so H is non-empty.

Now let $x, y \in H$. Then $x = s_1^{r_1} \cdots s_m^{r_m}$ and $y = t_1^{r_1} \cdots t_n^{r_n}$ where $s_i, t_j \in S$ for $i = 1, \ldots, m$ and $j = 1, \ldots, n$. Then

$$xy^{-1} = s_1^{r_1} \cdots s_m^{r_m} t_n^{-r_n} \cdots t_1^{-r_1} \in H.$$

Hence H is a subgroup as required. ■

Proposition 1.7

Let G be a group, let S be a non-empty finite subset of G and let

$$H = \{s_1^{r_1} \cdots s_n^{r_n} : n \in \mathbb{N}, s_i \in S, r_i \in \mathbb{Z}, i = 1, \ldots, n\}.$$

Then the subgroup generated by S is the whole of H, that is,

$$\langle S \rangle = H.$$

Proof By Lemma 1.6, the set H is a subgroup of G. Clearly the set contains S. Moreover, by closure, any subgroup containing S must contain all possible products of powers of S and so contain H. Hence $\langle S \rangle = H$ from Definition 1.3. ■

Exercise 1.10

Let $G = S_5$ and let $a = (1\,2\,3\,4\,5), b = (2\,5)(3\,4)$. Show that $bab^{-1} = a^4$ and hence that

$$H = \langle a, b \rangle = \{a^r b^s : r = 0, \ldots, 4, s = 0, 1\}.$$

Deduce that H is a subgroup of G of order 10.

2 Conjugates, centralisers and centres

Chapter 5 reminded you about conjugacy and normal subgroups. In Chapter 6 you saw that conjugation allows us to define a group action of D_6 on itself. This section looks at conjugation and related ideas in a little more detail.

As you may recall from your previous studies, conjugation brings out similarities between group elements. For example, in the symmetric group S_4 there are eight 3-cycles that can be regarded as being similar in some sense. In the dihedral group D_5 it is reasonable to regard all the reflections as being similar, but is the same true for the reflections in D_6? It is certainly the case that rotations in D_6 are not necessarily similar since they can have different orders. However, rotations of the same order are similar. One aim of this section is to formalise this notion of similarity. The ideas involved in this have some striking consequences for group theory in general.

2.1 Conjugates

Recall from Chapter 5, Definition 3.9, that two elements a and b of a group G are *conjugate* in G if there is $g \in G$ such that $b = gag^{-1}$. In this case, we also say that gag^{-1} is the **conjugate of a by g**. Conjugacy by a given element of G can be used to define an isomorphism of G to itself.

Proposition 2.1

Let G be a group and let $g \in G$. Then the function $\phi : G \to G$, which sends each element a to its conjugate by g, that is,

$$\phi : a \mapsto gag^{-1},$$

is an isomorphism.

Proof Let $a, b \in G$. Then

$$\phi(a)\phi(b) = gag^{-1}gbg^{-1} = gabg^{-1} = \phi(ab).$$

Thus ϕ is a homomorphism.

Now consider the function $\psi : G \to G$ defined by

$$\psi : a \mapsto g^{-1}ag;$$

that is, the function that maps a to its conjugate by g^{-1}. We have

$$\psi \circ \phi\,(a) = \psi(gag^{-1}) = g^{-1}(gag^{-1})g = a.$$

Similarly, $\phi \circ \psi\,(a) = a$, so ψ is the inverse for ϕ, hence ϕ is an isomorphism, as required. ■

In the following exercise, recall that the dihedral group D_n has presentation

$$D_n = \langle r, s \mid r^n = s^2 = e, sr = r^{n-1}s \rangle,$$

and each of its elements can be expressed in the standard form $r^i s^j$ for $i = 0, \ldots, n-1$ and $j = 0, 1$.

Exercise 2.1

Compute the following conjugates, giving your answers in standard form.

(a) srs^{-1} and rsr^{-1} in D_5

(b) srs^{-1} and rsr^{-1} in D_6

2.2 Conjugacy classes

In Chapter 6, Section 3, we saw how the orbits of a group action partition the set being acted on and so they define an equivalence relation. In Proposition 3.6 in the same chapter, we also saw that conjugation can be used to define an action of D_6 on itself. This action can be generalised to give an action of any group on itself. This is the action that we will look at in detail in this subsection.

Theorem 2.2

Let G be a group. Then G acts on G by the rule

$$g \wedge a = gag^{-1} \quad \text{for all } a, g \in G,$$

and we say that G **acts on itself by conjugation**.

Proof We check that the conditions in Definition 3.1 of Chapter 6 are satisfied. First of all, it is clear that $g \wedge a \in G$ for all $a, g \in G$. Moreover:

(a) $e \wedge a = eae^{-1} = a$ for every $a \in G$

(b) $(gh) \wedge a = ghah(gh)^{-1} = ghah^{-1}g^{-1} = g \wedge (hah^{-1}) = g \wedge (h \wedge a)$ for all $g \in G, h \in G$ and all $a \in G$. ■

The action defined in Theorem 2.2 partitions G into orbits whose elements are conjugate to each other, and thus similar in some sense. The orbits turn out to be certain familiar subsets of G that you met in Chapter 5: they are the conjugacy classes of G. Thus, in the context of actions by conjugation, conjugacy classes can be defined as follows.

Definition 2.3 *Conjugacy class*

Let G be a group and $a \in G$. Then the orbit of a in the action of G on itself by conjugation is written $\mathrm{Conj}_G(a)$ and it is called the **conjugacy class** of a in G. Thus

$$\mathrm{Conj}_G(a) = \{gag^{-1} : g \in G\}.$$

Example 2.4 *Conjugacy in S_3*

The symmetric group S_3 has three transpositions, $(1\,2), (1\,3)$ and $(2\,3)$, and two 3-cycles, $(1\,2\,3)$ and $(1\,3\,2)$.

If you calculate the conjugate $\sigma(1\,2)\sigma^{-1}$ for each $\sigma \in S_3$, you should obtain the three transpositions, each occurring twice.

The conjugates of $(1\,2\,3)$ are the two 3-cycles, and the only conjugate of the identity permutation is e itself. Thus, the conjugacy classes in S_3 are

$$\{(1\,2), (1\,3), (2\,3)\},\ \{(1\,2\,3), (1\,3\,2)\} \text{ and } \{e\}.$$

In Example 2.4, the conjugacy classes partition the group S_3. This is an instance of one of several general properties of conjugacy classes, the most important of which are given below. Most of these properties can be deduced from those of general equivalence classes.

Proposition 2.5

Let G be a group. Then:

(a) for each element a of G, $a \in \mathrm{Conj}_G(a)$

(b) for $a, b \in G$, $\mathrm{Conj}_G(a) = \mathrm{Conj}_G(b)$ if, and only if, b is a conjugate of a

(c) $\mathrm{Conj}_G(e) = \{e\}$ for any group G

(d) all the elements of a conjugacy class have the same order

(e) if G is finite of order n, then the number of elements in a conjugacy class must divide n.

Proof

(a) This holds because $a = eae^{-1}$.

(b) Suppose that b is a conjugate of a. Then $b = xax^{-1}$ for some $x \in G$, so $x^{-1}bx = a$. Now if $c \in \mathrm{Conj}_G(a)$, then $c = dad^{-1}$ for some $d \in G$ and so

$$c = dx^{-1}bxd^{-1} = (dx^{-1})b(dx^{-1})^{-1} \in \mathrm{Conj}_G(b).$$

Thus $\mathrm{Conj}_G(a) \subseteq \mathrm{Conj}_G(b)$. The reverse inclusion is proved similarly. This shows that if b is a conjugate of a, then $\mathrm{Conj}_G(a) = \mathrm{Conj}_G(b)$.

Now suppose that $\mathrm{Conj}_G(a) = \mathrm{Conj}_G(b)$. Then since $b \in \mathrm{Conj}_G(b)$ by statement (a), $b \in \mathrm{Conj}_G(a)$ and so b is a conjugate of a.

We have proved that $\mathrm{Conj}_G(a) = \mathrm{Conj}_G(b)$ if, and only if, b is a conjugate of a.

(c) This follows from the fact that $geg^{-1} = e$ for all $g \in G$.

(d) From Proposition 2.1 and Theorem 4.6 of Chapter 5, we see that a and gag^{-1} have the same order. The result follows.

(e) This follows from the Orbit–Stabiliser Theorem (Corollary 3.13 of Chapter 6), since a conjugacy class is an orbit under a group action. ■

Since any group G is partitioned into its conjugacy classes, when G is finite the total number of elements in G must be the sum of the numbers of elements in each conjugacy class. This gives the following theorem.

Theorem 2.6

Let G be a finite group and let $C_1, C_2, \ldots, C_k$ be its distinct conjugacy classes. Then

$$|G| = |C_1| + |C_2| + \cdots + |C_k|.$$

Proof This follows from the fact that the conjugacy classes of G partition the group (Proposition 3.11(b) of Chapter 5). ■

The equation in Theorem 2.6 is usually called the **class equation** for G. From Exercise 3.6 of Chapter 5 we see that the class equation for S_3 is

$$6 = 1 + 3 + 2.$$

When working out the conjugacy classes of a given group, you can speed up calculations by noting the following.

- Since the identity e commutes with every other element, its conjugacy class is the set $\{e\}$. More generally, if g is any group element that commutes with every other element, its conjugacy class is $\{g\}$.
- Since conjugacy classes are orbits, their size must divide the order of the group.

Exercise 2.2

For each of the following groups, find the conjugacy classes and hence write down the class equation.

(a) $D_4 = \{r^i s^j : i = 0, \ldots, 3,\ j = 0, 1;\ r^4 = s^2 = e,\ sr = r^3 s\}$

(b) $\mathrm{Dic}_2 = \{a^i b^j : i = 0, \ldots, 3,\ j = 0, 1;\ a^4 = e, a^2 = b^2, aba^3b = e\}$

Exercise 2.2(a) shows that in the dihedral group D_4, conjugacy distinguishes between the two reflections rs and $r^3 s$, which form one class, and the other two reflections, s and $r^2 s$. Depending on the choice of s, one pair will be reflections in the diagonals and the other pair reflections in the lines joining midpoints of opposite sides. The elements s and rs, both of order 2, are *not* conjugate in D_4.

2.3 Centralisers

We have seen that conjugation gives a group action whose orbits are the conjugacy classes. In this subsection we will look at the *stabilisers* of this action. Recall that the stabiliser of an element a of a group G consists of those elements g of G such that $gag^{-1} = a$.

Definition 2.7 *Centraliser*

Let G be a group and $a \in G$. Then the stabiliser of a in the action of G on itself by conjugation is called the **centraliser** of a in G and it is written $\mathrm{Cent}_G(a)$. Thus

$$\mathrm{Cent}_G(a) = \{g \in G : gag^{-1} = a\}.$$

If the group is clear from the context, the subscript G can be omitted from the notation $\mathrm{Cent}_G(a)$.

If $gag^{-1} = a$ then multiplying by g on the right gives $ga = ag$. Conversely, if $ga = ag$, then multiplying by g^{-1} on the right gives $gag^{-1} = a$. Therefore

$$gag^{-1} = a \quad \text{if, and only if,} \quad ga = ag.$$

Thus

$$\mathrm{Cent}_G(a) = \{g \in G : ga = ag\},$$

so in fact the centraliser of a in G consists of all the elements of G that commute with a.

Since $\mathrm{Cent}_G(a)$ is a stabiliser in a group action, it is always a subgroup of G (see Exercise 3.8 of Chapter 6). For example, in D_4 the centraliser of r must contain e, r, r^2, r^3, as all these elements commute with r. Since s does not commute with r, the centraliser of r cannot be the whole group. By Lagrange's Theorem, it must have order 1, 2, 4 or 8, so

$$\mathrm{Cent}_{D_4}(r) = \{e, r, r^2, r^3\}.$$

It is always true that $\langle a \rangle \subseteq \mathrm{Cent}_G(a)$, because $aa^i = a^{i+1} = a^i a$ for all integers i, but in the next exercise you will see examples where $\langle a \rangle \neq \mathrm{Cent}_G(a)$.

Exercise 2.3

Find the following centralisers. In each case, state whether $\mathrm{Cent}_G(a) = \langle a \rangle$.

(a) $\mathrm{Cent}_{S_3}(1\,2\,3)$ and $\mathrm{Cent}_{S_3}(1\,2)$

(b) $\mathrm{Cent}_{D_4}(r^2)$ and $\mathrm{Cent}_{D_4}(s)$

Exercise 2.4

(a) If G is an abelian group, what can you say about the centraliser of any element of G?

(b) What is the centraliser of the identity element e_G in any group G?

2.4 Centres

In Exercises 2.3 and 2.4, we saw examples where a centraliser $\mathrm{Cent}_G(a)$ is the whole group G. In other words, the element a commutes with every element of G. Such elements are important enough to deserve some specific terminology.

Definition 2.8 *Central elements*

Let G be a group, and let $a \in G$ be an element that commutes with every other element of G. Then a is said to be a **central element** in G.

The set of all central elements in G is called the **centre** of G and it is denoted by $Z(G)$. Thus

$$Z(G) = \{a \in G : ga = ag \text{ for all } g \in G\}.$$

An element a of G is central in G if, and only if, $a \in \mathrm{Cent}_G(g)$ for all $g \in G$. In other words, the centre of the group is the intersection of all the centralisers. From this description, it is possible to deduce that $Z(G)$ is a subgroup of G, but we will check this directly from the subgroup criterion, Proposition 2.4 of Chapter 5. Indeed, we will go a step further and show that $Z(G)$ is in fact a normal subgroup.

Proposition 2.9

Let G be a group. Then the centre $Z(G)$ is a normal subgroup of G.

Proof We first observe that if $xg = gx$, then multiplying both sides of the equation on the left and on the right gives

$$x^{-1}xgx^{-1} = x^{-1}gxx^{-1};$$

that is, $gx^{-1} = x^{-1}g$. Now:

- For all g in G, we have $ge = eg$, so $e \in Z(G)$ and $Z(G) \neq \emptyset$.
- Let $x, y \in Z(G)$. Thus, for all $g \in G$ we have $gx = xg$ and $gy = yg$. Then

  $$g(x^{-1}y) = (gx^{-1})y = (x^{-1}g)y = x^{-1}(gy) = x^{-1}(yg) = (x^{-1}y)g,$$

  thus $g(x^{-1}y) = (x^{-1}y)g$ for all $g \in G$. That is, $x^{-1}y \in Z(G)$.

Therefore $Z(G)$ is a subgroup of G by the subgroup criterion.

Now let $a \in Z(G)$ and $g \in G$. Then $gag^{-1} = a \in Z(G)$ so that $Z(G)$ is a normal subgroup of G by Proposition 3.7 of Chapter 5. ■

Exercise 2.5

Let G be a group with centre $Z(G)$ and let H be a subgroup of $Z(G)$. Show that H is a normal subgroup of G.

There are several different ways of saying that an element is central in a group. For convenience we list them in a proposition.

Proposition 2.10

Let G be a group and let $a \in G$. The following are equivalent ways of saying that a is central in G.

(a) $ga = ag$ for all $g \in G$

(b) $\mathrm{Cent}_G(a) = G$

(c) $a \in \mathrm{Cent}_G(g)$ for all $g \in G$

(d) $gag^{-1} = a$ for all $g \in G$

(e) $\mathrm{Conj}_G(a) = \{a\}$

The significance of some of these conditions will hopefully become clear as you meet more examples and results about conjugacy classes and centralisers: loosely speaking, having many conjugates in G is the opposite of commuting with many elements of G. This remark is justified by the equivalence between conditions (a) and (d) in Proposition 2.10: an element a is equal to its conjugate by g if, and only if, a and g commute.

The centre of an abelian group is the whole group. On the other hand, the centre of a group may be the trivial subgroup, as you can see in the next exercise. The order of the centre of a group, relative to the order of the whole group, is a measure of how close the group is to being abelian.

Exercise 2.6

(a) Write down the elements of S_3 that commute with $(1\,3)$, that is, write down $\mathrm{Cent}_{S_3}(1\,3)$.

(b) Hence find $Z(S_3)$.

2.5 Conjugates and centralisers

In Chapter 6, the Orbit–Stabiliser Theorem gave a connection between orbits and stabilisers. In the context of the action of a group G on itself by conjugation, the Orbit–Stabiliser Theorem gives a connection between conjugacy classes (the orbits) and centralisers (the stabilisers). In particular, when G is finite, the finite form of the theorem, namely

$$|\mathrm{Orb}_G(a)| \times |\mathrm{Stab}_G(a)| = |G|,$$

gives the formula below.

Theorem 2.11

For any element a of any finite group G,

$$|\mathrm{Conj}_G(a)| \times |\mathrm{Cent}_G(a)| = |G|.$$

Proof The result follows from the Orbit–Stabiliser Theorem (Corollary 3.13 of Chapter 6) and Theorem 2.2. ■

In particular, Theorem 2.11 tells us that $|\mathrm{Conj}_G(a)|$ is always a factor of $|G|$, and that it is inversely proportional to $|\mathrm{Cent}_G(a)|$. In a group where we have already calculated conjugacy classes, such as S_n, this result enables us to quickly calculate centralisers and centres.

Example 2.12 *Centralisers and centre in S_n*

You may remember from your previous studies that in S_n any two cycles of the same length are conjugate.

The number of different n-cycles in S_n is $(n-1)!$ and so the conjugacy class of the cycle $\sigma = (1\,2\,\ldots\,n)$ contains $(n-1)!$ elements.

σ is the Greek letter 'sigma'.

Hence the centraliser $\mathrm{Cent}(\sigma)$ has order

$$n = \frac{n!}{(n-1)!} = n,$$

and so $\mathrm{Cent}(\sigma)$ must be the cyclic subgroup $\langle(1\,2\,\ldots\,n)\rangle$.

Now let $\tau = (1\,2\,\ldots\,(n-1))$. The conjugates of τ in S_n are the cycles ρ of length $n-1$. How many of these are there? There are n choices for the number that does not appear in ρ and, for each of these, there are $(n-2)!$ different $(n-1)$-cycles. Thus τ has $n \times (n-2)!$ conjugates and so its centraliser has order $n-1$.

τ is the Greek letter 'tau'.

ρ is the Greek letter 'rho'.

Any element in the centre of S_n must commute with both σ and τ, and so must be in $\mathrm{Cent}(\sigma) \cap \mathrm{Cent}(\tau)$. As the highest common factor of n and $n-1$ is 1, it follows that

$$\mathrm{Cent}(\sigma) \cap \mathrm{Cent}(\tau) = \{e\}.$$

Consequently, the centre of S_n is the trivial subgroup $\{e\}$.

Exercise 2.7

Recall that Dic_2 has presentation

$$\mathrm{Dic}_2 = \langle a, b \mid a^4 = e, a^2 = b^2, aba^3b = e \rangle.$$

The conjugacy classes are as follows:

$$\{e\}, \{a^2\}, \{a, a^3\}, \{ab, a^3b\}, \{b, a^2b\}.$$

(a) Write down $Z(\mathrm{Dic}_2)$.

(b) Write down $\mathrm{Conj}_{\mathrm{Dic}_2}(a)$.

(c) Hence find $\mathrm{Cent}_{\mathrm{Dic}_2}(a)$.

Theorem 2.11 and the class equation have a striking theoretical consequence. We have just seen that certain familiar groups have trivial centres. However, sometimes the nature of the order of the group precludes this possibility.

Theorem 2.13

Let G be a group of prime power order, that is,

$$|G| = p^n$$

for some prime number p and positive integer n.

Then G has a non-trivial centre.

Proof Let $C_1, C_2, \ldots, C_k$ be a list of the different conjugacy classes of G, numbered so that $C_1 = \mathrm{Conj}_G(e) = \{e\}$. Thus $|C_1| = 1$. We aim to show that there is at least one other conjugacy class with a single element a, say, $a \neq e$ so that a is central by Proposition 2.10.

The class equation for G says that $p^n = 1 + |C_2| + |C_3| + \cdots + |C_k|$.

By Theorem 2.11, each $|C_i|$ is a factor of $|G| = p^n$. As p is prime, the only factors of p^n are $1, p, p^2, \ldots, p^{n-1}$ and p^n. It is impossible for $|C_2|, |C_3|, \ldots, |C_k|$ all to be multiples of p because, if they were, then 1 would be a multiple of p. Hence $|C_i| = 1$ for some $i > 1$. As noted above, if $C_i = \{a\}$ then $a \neq e$ and a is central. Thus $Z(G) \neq \{e\}$. ■

A group to which this theorem can be applied is D_4, whose order is the prime power $8 = 2^3$. The theorem tells us that, in contrast to S_4, the dihedral group D_4 must have non-trivial centre. The element r^2 is central, and the class equation for D_4 is

$$8 = 1 + 1 + 2 + 2 + 2.$$

The idea behind the proof of Theorem 2.13 is illustrated by the fact that it is impossible to express 8 as a sum of 1s, 2s, 4s and 8s with exactly one 1.

2.6 Groups of order p^2

This subsection provides an example of the role of quotient groups in group theory: we will use certain quotients to prove that whenever p is a prime number, all groups of order p^2 are abelian.

The basic idea in using quotient groups is to obtain information about a group G from a normal subgroup N and the quotient G/N. We will do this in the case where N is the centre of G. The group $Z(G)$ is abelian because any element of $Z(G)$ commutes with every element of G, and hence with every element of $Z(G)$. Moreover, we know from Proposition 2.9 that $Z(G)$ is normal, hence we can form the quotient group $G/Z(G)$.

Theorem 2.14

If G is a group such that $G/Z(G)$ is cyclic, then G is abelian.

Proof Let $Z = Z(G)$ and let gZ be a generator of G/Z. Then every element of G/Z, that is every coset of Z, has the form $(gZ)^m = g^m Z$ for some $m \in \mathbb{Z}$. But the cosets of Z give a partition of G, so each element a of G is in one of these. If $a \in g^m Z$, then $a = g^m z$ for some $m \in \mathbb{Z}$.

Now let $a, b \in G$. Then $a = g^{m_1} z_1$ and $b = g^{m_2} z_2$ for some $m_1, m_2 \in \mathbb{Z}$ and some $z_1, z_2 \in Z$. Since z_1 and z_2 commute with every element of G and powers of g commute with each other,

$$ab = g^{m_1+m_2} z_1 z_2 = ba.$$

Thus G is abelian. ■

Theorem 2.15

If p is a prime number, then every group G of order p^2 is abelian.

Proof Let Z be the centre of G. We have to show that $Z = G$.

By Lagrange's Theorem, $|Z|$ must be one of 1, p, p^2, as these are the only factors of p^2. By Theorem 2.13, the centre Z is non-trivial; that is, $|Z| \neq 1$.

Suppose that $|Z| = p$. The quotient group G/Z has order $\frac{p^2}{p} = p$. Then G/Z is cyclic by Exercise 4.8 of Chapter 5. Theorem 2.14 then says that G must be abelian, that is $|Z| = |G| = p^2$, which contradicts the assumption $|Z| = p$. Thus the possibility $|Z| = p$ does not arise.

The only remaining possibility is that $|Z| = p^2$ and so $Z = G$. Hence G is abelian. ■

3 Groups of small order

This section classifies all groups of order up to 14, as well as all those groups whose order is a prime, twice a prime or the square of a prime. In other words, for these orders, we give a list of groups such that every group of one of those orders is isomorphic to one of the groups in the list. In order to achieve the classification, we will use the following theorems:

- from Chapter 5, Lagrange's Theorem and its consequences that the order of any element of a finite group G divides $|G|$ and that every group of prime order is cyclic
- from Chapter 6, Cauchy's Theorem (Theorem 3.16) and Theorem 1.5 on recognising direct products
- from this chapter, Theorem 2.15, which tells us that every group whose order is a square of a prime is abelian.

3.1 Groups of order p

Let p be a prime number and G be a group of order p. Then G is cyclic by Exercise 4.8 of Chapter 5. Thus we have the following proposition.

Proposition 3.1

Let p be a prime number and G be a group of order p. Then

$G \cong \mathbb{Z}_p$.

This proposition applies to all groups of orders 2, 3, 5, 7, 11 and 13.

3.2 Groups of order p^2 revisited

Let p be a prime number. We know from Theorem 2.15 that all groups of order p^2 are abelian. We also know from Theorem 3.19 of Chapter 6 that all abelian groups of order p^2 are direct products of cyclic groups. Therefore we have the following result.

Theorem 3.2

Let p be a prime number. Then every group of order p^2 is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Proof Let G be a group of order p^2. Then G is abelian by Theorem 2.15.

If G is cyclic, then $G \cong \mathbb{Z}_{p^2}$.

If G is not cyclic, it is a direct product of proper cyclic subgroups by Theorem 3.19 of Chapter 6. Any non-trivial proper subgroup of G must have order p and so be isomorphic to $\mathbb{Z}_p$. Hence $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$. ■

Theorem 3.2 applies in particular to groups of orders 4 and 9.

3.3 Groups of order $2p$

Among the groups whose order is less than or equal to 14, we do not yet have a classification for those of order 6, 10 and 14. These orders all have the form $2p$, where p is an odd prime.

We have already met some groups of order $2p$, for example the cyclic group $\mathbb{Z}_{2p}$, the direct product $\mathbb{Z}_p \times \mathbb{Z}_2$ and the dihedral group D_p. Theorem 2.11 of Chapter 6 tells us that

$$\mathbb{Z}_{2p} \cong \mathbb{Z}_p \times \mathbb{Z}_2,$$

so our known examples of non-isomorphic groups of order $2p$ only really include $\mathbb{Z}_{2p}$ and D_p.

The aim of this subsection is to show that any non-cyclic group of order $2p$ is isomorphic to the dihedral group D_p.

We start by looking at certain basic properties of the dihedral group D_n of order $2n$. At the beginning of this chapter we remarked that

$$D_n = \{r^i s^j : \ i = 0, \ldots, n-1, \ j = 0, 1; \ r^n = s^2 = e, \ sr = r^{n-1}s\}.$$

Lemma 3.3

Let G be a group of even order $2n$. Suppose that G has an element a of order n and an element b of order 2 with $b \notin \langle a \rangle$. Then:

(a) $bab^{-1} = a^k$ for some integer k such that $0 < k < n$ and n is a factor of $k^2 - 1$

(b) if $n \geq 3$ and $bab^{-1} = a^{n-1}$, then $G \cong D_n$.

Proof Let $H = \langle a \rangle$. Then H has order n and index 2 in G.

(a) Exercise 3.3 of Chapter 5 tells us that H is normal in G. So $bab^{-1} \in H$, and

$$bab^{-1} = a^k$$

for some integer k with $0 \leq k < n$.

Clearly $k \neq 0$, for otherwise $ba = b$ and $a = e$. Now b has order 2 so

$$b^2 = b^{-2} = e.$$

Therefore
$$\begin{aligned} a = b^2ab^{-2} &= b(bab^{-1})b^{-1} \\ &= b(a^k)b^{-1} \\ &= (bab^{-1})^k \\ &= (a^k)^k = a^{k^2}. \end{aligned}$$

Multiplying both sides of this equality on the right by a^{-1} gives $e = a^{k^2-1}$. As a has order n, it follows from Proposition 4.5 of Chapter 5 that n divides $k^2 - 1$.

(b) As H has index 2 in G, it only has two cosets in G. One of these is H and, because $b \notin H$, the other must be bH. Each element of G must be in H or bH so must be of the form a^i or of the form ba^i for some integer i with $0 \leq i < n$.

Because $bab^{-1} = a^{n-1}$ and $b^{-1} = b$, we have that $ab = ba^{n-1}$. As for the dihedral group, we can use the formula $ab = ba^{n-1}$ to express the product of any two elements of G in one of the forms a^i or a^ib.

It follows that the bijection $\phi : G \to D_n$ given by

Check that ϕ is a bijection.

$$\phi(a^i) = r^i \quad \text{and} \quad \phi(a^ib) = r^is$$

is an isomorphism. ■

Exercise 3.1

Let G be a group of order $2n$, where n is odd. Suppose that G has an element a of order n and an element b of order 2 and that $ab = ba$.

Show that the order of ab is $2n$.

Hint: use Lemma 2.7 of Chapter 6.

Theorem 3.4

If p is an odd prime, then every group of order $2p$ is isomorphic to either $\mathbb{Z}_{2p}$ or D_p.

Proof Let G be a non-cyclic group of order $2p$. By Cauchy's Theorem (Theorem 3.16 of Chapter 6), G has an element a of order p and an element b of order 2. Then $b \notin \langle a \rangle$ because its order, 2, is not a factor of $p = |\langle a \rangle|$.

By Lemma 3.3(a), we have $bab^{-1} = a^k$ where $0 < k < p$ and p divides $k^2 - 1 = (k+1)(k-1)$. As p is prime, either p divides $k+1$ or p divides $k-1$. Because $1 \leq k \leq p-1$, we have $p \geq k+1$ and so p cannot divide $k-1$. Thus the only possibilities are $k = p-1$ and $k = 1$.

If $k = 1$ then $ab = ba$, and so ab has order $2p$ by Exercise 3.1. In this case, $G = \langle ab \rangle \cong \mathbb{Z}_{2p}$ is cyclic.

If $k = p-1$, then Lemma 3.3(b) ensures that $G \cong D_p$. ■

Theorem 3.4 shows that all groups of order 6 are isomorphic to either $\mathbb{Z}_6$ or D_3, that all groups of order 10 are isomorphic to either $\mathbb{Z}_{10}$ or D_5, and that all groups of order 14 are isomorphic to either $\mathbb{Z}_{14}$ or D_7.

3.4 Groups of order 8

So far we have met five groups of order 8: the cyclic group $\mathbb{Z}_8$, the direct products $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, the dihedral group D_4 and the quaternion group Dic_2. We now find out whether there are any other possibilities.

Let G be a group of order 8. The possible orders of elements of G are 1, 2, 4 and 8. If $g \in G$ has order 4 or 8, then either g^2 or g^4 has order 2, so G has at least one element of order 2. Alternatively, Cauchy's Theorem gives the same conclusion. We now consider several cases.

Case 1

If G has an element g of order 8 then $G = \langle g \rangle$ is cyclic, that is,

$$G \cong \mathbb{Z}_8.$$

Case 2

Suppose that, apart from e, every element of G has order 2. Then every element of G is its own inverse and, for $a, b \in G$,

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba;$$

hence G is abelian.

If $a \neq e$ and $b \notin \langle a \rangle$ then G contains a subgroup $H = \{e, a, b, ab\}$ that is isomorphic to the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$. Let $K = \langle c \rangle$, where c is any of the four elements of $G \setminus H$. Then, by Proposition 1.9 of Chapter 6,

Recall that $G \setminus H = \{g \in G : g \notin H\}$.

$$G = HK \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Case 3

Suppose that G has an element a of order 4 and an element b of order 2 such that $b \notin \langle a \rangle$. By Lemma 3.3(a), we know that $bab^{-1} = a^j$ for some j such that $0 < j < 4$ and 4 divides $j^2 - 1$. The only possibilities are $j = 1$ and $j = 3$.

If $j = 3$ then $G \cong D_4$ by Lemma 3.3(b).

If $j = 1$ then $ba = ab$ and, setting $K = \langle b \rangle$ and applying Proposition 1.9 of Chapter 6, we get

$$G = HK \cong \mathbb{Z}_4 \times \mathbb{Z}_2.$$

The above cases cover all the groups of order 8 listed at the beginning of the subsection, apart from Dic_2. The next proposition shows that the only group of order 8 missing from our initial list is indeed Dic_2.

Proposition 3.5

Let G be a group of order 8 that is not isomorphic to any of the groups $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and D_4. Then G has exactly one element d of order 2 and six elements

$$a^{\pm 1},\ b^{\pm 1} \text{ and } c^{\pm 1}$$

of order 4.

Moreover, $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$ and $ba = a^3b$.

Proof As $G \ncong \mathbb{Z}_8$, it has no element of order 8. Moreover, G must have at least one element, a say, of order 4, otherwise Case 2 would apply to give $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Let $d = a^2$ and let g be any element of order 2. Then $g \in \langle a \rangle$, otherwise we would have the situation of Case 3 and $G \cong D_4$ or $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

The only element of $\langle a \rangle$ of order 2 is d, so $g = d$. Hence the only element of G of order 2 is d and there are six elements of order 4, which must occur as three pairs of inverse elements, say $a^{\pm 1}$, $b^{\pm 1}$ and $c^{\pm 1}$.

Let $H = \langle a \rangle = \{e, a, a^2, a^3\}$. As H has index 2 in G, it only has two right cosets in G. One of these is H and, because $b \notin H$, the other must be

$$Hb = \{b, ab, a^2b, a^3b\}.$$

Since $G = H \cup Hb$, we get

$$G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

as required. Notice that $d = a^2 = b^2$, $b^{-1} = b^3 = b^2b = db = a^2b$, and c must be either ab or a^3b.

Hence $(ab)^2 = d = a^2$, that is, $abab = a^2$. By cancellation,

$$bab = a$$

and so $ba = ab^{-1} = a^3b$. ■

Proposition 3.5 shows that, up to isomorphism, there is at most one group of order 8 not included in the three cases listed at the beginning of this subsection.

If such a group exists, then its elements satisfy the conditions in Proposition 3.5. But these conditions are precisely those we get from the standard form of the dicyclic group of order 8, Dic_2, introduced in Subsection 1.2. In particular, the elements satisfy the relations

$$a^4 = e = b^4,\ a^2 = b^2 (= d) \text{ and } ba = ab^{-1} = a^3b,$$

which is equivalent to $aba^3b = e$ (see Exercises 1.6 and 1.8). Hence such a group is again isomorphic to a group that we have already met.

Together with the case-by-case analysis that preceded it, Proposition 3.5 gives the following classification theorem for groups of order 8.

Theorem 3.6

Every group G of order 8 is isomorphic to one of the five groups

$$\mathbb{Z}_8,\ \mathbb{Z}_4 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ D_4,\ \mathrm{Dic}_2.$$

3.5 Groups of order 12

We now show that, up to isomorphism, there are five groups of order 12.

Exercise 3.2

Show that $D_3 \times \mathbb{Z}_2 \cong D_6$.

Exercise 3.3

Show that S_4 has only one subgroup of order 12.

Hint: use the sizes of conjugacy classes in S_4 and the fact that a subgroup of order 12 must be normal.

The next proposition gives a classification of *abelian* groups of order 12.

Proposition 3.7

Let G be an abelian group of order 12. Then either $G \cong \mathbb{Z}_6 \times \mathbb{Z}_2$ or $G \cong \mathbb{Z}_{12}$.

Proof By Cauchy's Theorem, G has an element a of order 2 and an element b of order 3. Since $ab = ba$, the product ab has order 6, so $\langle ab \rangle$ is a normal subgroup and $\langle b \rangle$ is a subgroup of $\langle ab \rangle$.

Let $d \in G$ with $d \notin \langle ab \rangle$. We know that d has order 2, 3, 4, 6 or 12.

If d has order 2, then Proposition 1.9 in Chapter 6 gives

$$G = HK \cong \mathbb{Z}_6 \times \mathbb{Z}_2,$$

where $H = \langle ab \rangle$ and $K = \langle d \rangle$.

If d has order 3, then G has a subgroup $\langle b \rangle \times \langle d \rangle$ of order 9, which contradicts Lagrange's Theorem. Therefore this possibility does not arise.

If d has order 4, then bd has order 12, and $G = \langle bd \rangle$ is cyclic; that is,

$$G \cong \mathbb{Z}_{12}.$$

If d has order 12 then $G = \langle d \rangle \cong \mathbb{Z}_{12}$.

We are left with the possibility that all elements d of G that are not in $\langle ab \rangle$ have order 6. If d has order 6, then d^2 and d^3 have orders 3 and 2 respectively, and so they must be in $\langle ab \rangle$.

Hence

$$d = d^3 d^{-2} \in \langle ab \rangle,$$

contradicting the choice of d.

Thus if G is abelian of order 12, either $G \cong \mathbb{Z}_6 \times \mathbb{Z}_2$ or $G \cong \mathbb{Z}_{12}$. ■

We are now left to find out what the *non*-abelian groups of order 12 are.

Proposition 3.8

Let G be a non-abelian group of order 12, and let a and b be elements of G such that:

(a) a has order 6

(b) b has order 2

(c) $b \notin \langle a \rangle$.

Then $G \cong D_6$.

Proof By Lemma 3.3(a), we know that

$$bab^{-1} = a^j$$

for some j such that $0 < j < 6$, and 6 divides $j^2 - 1$. The only possibilities are $j = 1$ and $j = 5$.

If $j = 1$, then $bab^{-1} = a$ gives $ba = ab$. Then

$$G = \langle a \rangle \langle b \rangle \cong \mathbb{Z}_6 \times \mathbb{Z}_2,$$

which is abelian.

Hence $j = 5$ and, by Lemma 3.3(b), $G \cong D_6$. ■

In the next result we are going to use the notion of the *kernel of a group action*. Let G be a group acting on a set X by an action $\wedge$, and let S_X denote the group of permutations of X. The action gives rise to a homomorphism $\phi : G \to S_X$, where the image of an element g of G is the permutation ϕ_g of X defined by

$$\phi_g(x) = g \wedge x \quad \text{for all } x \in X.$$

The defining properties of a group action ensure that ϕ is a homomorphism. The kernel of this homomorphism is called the **kernel of the action** $\wedge$ and it is denoted by $\ker \wedge$. An element g of G is in $\ker \wedge$ if ϕ_g is the identity permutation, so that

$$\ker \wedge = \{g \in G : g \wedge x = x \text{ for all } x \in X\}.$$

Thus $\ker \wedge$ is the set of those elements of G that stabilise *every* element of X. In particular, $\ker \wedge = \bigcap_{x \in X} \mathrm{Stab}(x)$.

Since $\ker \wedge$ is the kernel of a group homomorphism, it is a normal subgroup of G by Theorem 4.11 of Chapter 5.

Check for yourself that $\phi : G \to S_X$ is a group homomorphism.

Proposition 3.9

Let G be a group of order 12. Then:

(a) If G has a subgroup H of order 3 that is not normal, then $G \cong A_4$.

(b) If G has no element of order 6, then $G \cong A_4$.

Proof

(a) The group G acts on the set X of left cosets of H in G by

$$g \wedge aH = (ga)H.$$

Since the index of H in G is 4, the set X contains four elements. If we number these elements from 1 to 4, a permutation of X can be viewed as a permutation of the set $\{1, 2, 3, 4\}$, that is, as an element of S_4, and S_X is isomorphic to S_4.

The kernel K of this action is contained in $H = \mathrm{Stab}(H)$, and it is a normal subgroup of G. Since the order of H is prime, H has only two subgroups, namely H and $\{e\}$, and it is not itself normal in G. Therefore $K = \{e\}$.

We have observed that $S_X \cong S_4$, therefore ϕ can be viewed as a homomorphism from G to S_4 whose kernel is K. By the First Isomorphism Theorem, the group G is isomorphic to its image $\phi(G)$, which is isomorphic to a subgroup of S_4 of order 12.

We have seen from Exercise 3.3 that S_4 only has one subgroup of order 12, namely A_4. Therefore $\phi(G) = A_4$ and $G \cong A_4$.

(b) By Cauchy's Theorem, G has an element a of order 3.

Let $H = \langle a \rangle$ and suppose that H is normal. Then

$$bab^{-1} \in H = \{e, a, a^2\}$$

for all $b \in G$. The possibility $bab^{-1} = e$ cannot occur because $a \neq e$, so $bab^{-1} = a$ or a^2.

The centraliser $\mathrm{Cent}(a)$ of a in G is a subgroup of G containing H so, by Lagrange's Theorem, it has order 3, 6 or 12.

If it has order 6 or 12 then, by Cauchy's Theorem, it has an element g, say, of order 2. As $ag = ga$, the element ag would have order 6. As G has no such element, we must have $|\mathrm{Cent}(a)| = 3$ and hence

$$\mathrm{Cent}(a) = H.$$

Let $b, c \in G \setminus H$. Then $b \notin \mathrm{Cent}(a)$, so $ba \neq ab$ and hence $bab^{-1} \neq a$. Therefore $bab^{-1} = a^2$ and $ba = a^2b$. Similarly $ca = a^2c$.

Now consider bc. We have

$$bca = ba^2c = (ba)ac = a^2(ba)c = a^2a^2bc = a^4bc = abc,$$

thus $bc \in \mathrm{Cent}(a) = H$ for all $b, c \in G \setminus H$. But for each $b \in G \setminus H$, the nine different elements $c \in G \setminus H$ give rise, by the cancellation laws, to nine different elements bc. These cannot all be in H. Hence H cannot be normal and so, by part (a), $G \cong A_4$. ■

Proposition 3.10

Let G be a group of order 12 that is not isomorphic to any of the groups $\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, D_6, A_4. Then G is not abelian, and it has an element b of order 6 such that every element of order 2 in G is in $\langle b \rangle$.

Moreover, G has two elements b and b^{-1} of order 6, two elements of order 3, one element $d = b^3$ of order 2, and six elements of order 4.

Proof Proposition 3.7 shows that G is not abelian. Proposition 3.9(b) shows that G has an element b of order 6, and Proposition 3.8 shows that every element of order 2 in G is in $\langle b \rangle$. So G has a unique element $d = b^3$ of order 2.

This is reminiscent of the situation in Proposition 3.5.

Let $H = \langle b \rangle$ and note that, in H:

- e has order 1
- b has order 6
- b^2 has order 3
- $b^3 = d$ has order 2
- b^4 has order 3
- $b^5 = b^{-1}$ has order 6.

We will show that the six elements of G not in H must all have order 4. To see this, let $a \in G$ with $a \notin H$. Then a cannot have order 2 because the only element of G of order 2 is in H. Moreover, G is not abelian, hence not cyclic, so no element has order 12. Therefore a has order 3, 4 or 6.

As H has index 2, it is normal in G, and H and aH are the only cosets of H in G. It follows that every element of G has one of the forms b^i or ab^i.

As G is not abelian, $ab \neq ba$, otherwise all pairs of elements commute. Since H is normal, $aba^{-1} \in H$ and, because $ab \neq ba$, we have $aba^{-1} \neq b$. Conjugation by a is an isomorphism by Proposition 2.1, so aba^{-1} has the same order as b and so it must be the other element of H of order 6, namely $aba^{-1} = b^5 = b^{-1}$. Note this also means that $ab^{-1}a^{-1} = (aba^{-1})^{-1} = (b^{-1})^{-1} = b$.

If a has order 3 or 6, then $a^3 = e$ or $a^3 = b^3 = d$, the unique element of order 2 in G. In both cases we have $a^3ba^{-3} = b$. However, we also have

$$a^3ba^{-3} = a^2b^{-1}a^{-2} = aba^{-1} = b^{-1}.$$

Hence it is impossible for a to have order 3 or 6 and a must have order 4.

To summarise, G has two elements b and b^{-1} of order 6, two elements of order 3, one element $d = b^3$ of order 2 and six elements of order 4, as required. ■

The next exercise shows that Dic_3 has the properties described in Proposition 3.10. Then Exercise 3.5 will give sufficient information to construct the Cayley table of any group of order 12 not covered by Propositions 3.7, 3.8 and 3.9, and shows that such a group must satisfy the conditions of Proposition 3.10. These two exercises complete the classification of groups of order 12.

Exercise 3.4

Show that the dicyclic group Dic_3 has two elements of order 6, two elements of order 3, one element of order 2 and six elements of order 4.

Exercise 3.5

Let G be any group of order 12 not isomorphic to any of the groups $\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, D_6, A_4, so that the numbers of elements in G of orders $2, 3, 4$ and 6 are $1, 2, 6$ and 2 respectively.

Let a and b be elements of G with orders 4 and 6 respectively. Show that ab has order 4 and hence that $(ab)^2 = a^2$. Deduce that $ba = ab^{-1} = a^3b^2$, and hence show that $aba^3b = e$ and that G is Dic_3.

Hint: $a^2 = b^3$ is the unique element of order 2.

The propositions and exercises in this section give the following classification theorem for groups of order 12.

Theorem 3.11

Every group G of order 12 is isomorphic to one of the five groups

$$\mathbb{Z}_{12},\ \mathbb{Z}_6 \times \mathbb{Z}_2,\ A_4,\ D_6,\ \mathrm{Dic}_3.$$

Table 3.1 summarises the results we have obtained for groups of order up to and including 14.

Table 3.1 Groups of order up to and including 14

Order of group	Possible groups
1	$\mathbb{Z}_1 = \{e\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6$, $D_3 (\cong S_3)$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_4, Dic_2
9	$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$
10	$\mathbb{Z}_{10}$, D_5
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, A_4, D_6, Dic_3
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14}$, D_7

4 Finite p-groups

This section investigates a particular class of groups: those whose order is a power of a prime. A key tool in the investigation is Theorem 2.14, which shows that if the quotient of a group by its centre is cyclic, then the group is abelian.

In this section, p will always denote a prime number.

4.1 p-groups and their subgroups

In Subsection 3.2 we saw that any group whose order is the square of a prime is abelian and isomorphic to a direct product of cyclic groups. This result does not generalise to groups whose order is any power of a prime, but we will see that this more general condition still has some important consequences for the structure of the group.

Definition 4.1 *Finite p-group*

Let p be a prime and n a positive integer. Then a group of order p^n is called a **p-group**.

In Theorem 2.15 we considered the case where $n = 2$ and we showed that groups of order p^2 are abelian.

While groups of order p^2 must be abelian, the situation is rather more complicated for groups of order p^3 – you need only consider the discussion

about groups of order 8 in Subsection 3.4 to realise this. This discussion produced three abelian and two non-abelian groups of order $2^3 = 8$. The non-abelian ones are the dihedral group D_4 and the dicyclic group Dic_2.

Theorem 2.13 tells us that the centre of a p-group must be non-trivial. This result does give *some* information about groups of order p^3: the centre $Z(G)$ of such a group G can only have order p, p^2 or p^3.

Exercise 4.1

Let G be a group of order p^3. Show that $Z(G)$ cannot have order p^2.

We have now reduced the possibilities for $|Z(G)|$ to p and p^3.

If the order of $Z(G)$ is p^3, the group G is abelian and Theorem 3.19 of Chapter 6 tells us that G is a direct product of cyclic groups, so G must be isomorphic to one of

$$\mathbb{Z}_{p^3}, \quad \mathbb{Z}_p \times \mathbb{Z}_{p^2} \quad \text{or} \quad \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p.$$

If the order of $Z(G)$ is p, then the quotient group $G/Z(G)$ has order p^2, so it is abelian by Theorem 2.15. It follows that $G/Z(G)$ may only be isomorphic to one of

$$\mathbb{Z}_{p^2} \quad \text{or} \quad \mathbb{Z}_p \times \mathbb{Z}_p.$$

However, if the quotient were $\mathbb{Z}_{p^2}$, we would have a cyclic quotient, so G would be abelian and the order of the centre would be p^3 and not p.

We conclude that a non-abelian group G of order p^3 has a centre of order p and that $G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Unfortunately, this information does not uniquely determine the structure of G. For example, this discussion shows that any non-abelian group G of order 8 has a centre of order 2 and that the quotient by the centre is $\mathbb{Z}_2 \times \mathbb{Z}_2$. However, we know that there are two different non-abelian groups of order 8, and they must both satisfy these conditions.

This example shows that knowing the structure of a normal subgroup and the structure of the corresponding quotient group is not, in general, sufficient to determine the structure of the group itself.

It turns out that p-groups have an important structural property: a group of order p^n has a subgroup of order p^k for each positive $k \leq n$. In fact, a little more is true and the full result is contained in Theorem 4.3 below. First we give a lemma that is needed for the proof in the abelian case.

Lemma 4.2

Let G be an abelian p-group of order p^n for some positive integer n, with $n \geq 2$. Then G has a subgroup of order p^{n-1}.

Proof The proof is by induction on n.

If $n = 2$, by Cauchy's Theorem G has an element of order p, which generates a subgroup of order p.

Now assume that every abelian group of order p^k, where $k > 2$, has a subgroup of order p^{k-1}.

Suppose that G has order p^{k+1}. Then G has a subgroup H, say, of order p by Cauchy's Theorem. Since G is abelian, H is normal in G. The quotient group G/H is abelian and it has order

$$\frac{|G|}{|H|} = p^k.$$

By the induction hypothesis, G/H has a subgroup of order p^{k-1}. By the Correspondence Theorem (Theorem 4.17 of Chapter 5), we know this subgroup must have the form K/H for some subgroup K of G. But now

$$|K/H| = \frac{|K|}{|H|} = \frac{|K|}{p} = p^{k-1},$$

which implies that K has order p^k. ■

Theorem 4.3

Let G be a p-group of order p^n for some positive integer n. Then there exist normal subgroups

$$\{e\} = H_0, H_1, \ldots, H_n = G$$

of G such that

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_{n-1} \subset H_n = G,$$

where $|H_i| = p^i$ for $i = 0, \ldots, n$.

Because of the set inclusions involving the H_i, we say that the H_i form a *chain* of subgroups.

Proof The proof is by induction on n.

For $n = 1$, the order of G is p and the required chain is simply

$$\{e\} = H_0 \subset H_1 = G.$$

We have $|H_i| = p^i$ for $i = 0, 1$ and the normality condition is trivially true.

Now assume that the theorem is true for all groups of order p^r, where $r \leq k$, and let G have order p^{k+1}.

If G is abelian, then, since p^k divides p^{k+1}, G has a subgroup H_k of order p^k by Lemma 4.2. By the induction hypothesis, H_k has a chain of subgroups with the correct orders:

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_{k-1} \subset H_k.$$

Combining this with $H_k \subset H_{k+1} = G$, we obtain the required chain:

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_k \subset H_{k+1} = G.$$

Since G is abelian, normality is automatic.

Now we consider the case where G is *not* abelian. Our strategy is to use what we know about the centre of a p-group to construct the chain of subgroups in two stages: from the trivial subgroup to the centre and then from the centre to the whole group.

Since G is non-abelian, its centre $Z(G)$ is not the whole group and so its order is *less* than p^{k+1}. By Lagrange's Theorem, $Z(G)$ is a p-group. So $|Z(G)| = p^s$, where $0 \leq s \leq k$, and we may apply the induction hypothesis to $Z(G)$.

Thus, there exists a chain of subgroups

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_s = Z(G)$$

of $Z(G)$ where $|H_i| = p^i$ for $i = 0, \ldots, s$. These subgroups are also subgroups of G. Furthermore, by Exercise 2.5, they are normal subgroups of G.

We now have the part of the required chain from the trivial subgroup to $Z(G)$, and we turn to completing the chain from $Z(G)$ to G.

To apply the induction hypothesis, we need another p-group of order less than p^{k+1}. The one we will use is the quotient of G by its centre.

Since G is a p-group, Theorem 2.13 tells us that $Z(G)$ has at least p elements. Hence

$$|Z(G)| = p^s, \quad 1 \leq s.$$

Since $Z(G)$ is normal in G, we may consider the quotient group $G/Z(G)$, whose order is

$$p^{k+1}/p^s = p^{k+1-s} \leq p^k.$$

Hence the quotient is a p-group to which we may apply the induction hypothesis. It follows that there exists a chain of normal subgroups of the quotient,

$$\{Z(G)\} = K_0 \subset K_1 \subset \cdots \subset K_{k+1-s} = G/Z(G),$$

where $|K_i| = p^i$, $i = 0, \ldots, k+1-s$.

To complete the proof, we must show that the chain of normal subgroups in the quotient group $G/Z(G)$ may be used to define a chain of normal subgroups of G between $Z(G)$ and G. The fact that we can do so is an immediate consequence of the Correspondence Theorem (Theorem 4.17 of Chapter 5), which tells us that each normal subgroup K_i of $G/Z(G)$ gives rise to a normal subgroup H_{i+s} of G that contains $Z(G)$. Since the correspondence is one–one and the K_is are all distinct, so are the H_{i+s}s. Moreover, the trivial subgroup K_0 of the quotient group corresponds to $Z(G) = H_s$.

The proof of the Correspondence Theorem shows that set inclusion is preserved by the correspondence. Hence we have a chain of normal subgroups

$$Z(G) = H_s \subset H_{s+1} \subset \cdots \subset H_{k+1} = G.$$

We know that $|Z(G)| = p^s$ and $|G| = p^{k+1}$, and also that there are $k - s$ subgroups in the (strictly inclusive) chain *between* $H_s = Z(G)$ and $H_{k+1} = G$, each of order p^i for some i. Therefore we must have $|H_i| = p^i$ for $i = s, \ldots, k+1$.

We have now constructed a chain of normal subgroups

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_s = Z(G) = H_s \subset \cdots \subset H_{k+1} = G$$

for G, where $|H_i| = p^i$, $i = 0, \ldots, k+1$, completing the inductive step. ■

4.2 Soluble groups

We have just shown that finite p-groups have a chain of normal subgroups, each contained in the next. Under certain conditions, a chain of subgroups satisfying some additional requirements is enough to pin down a group up to isomorphism. Thus, finding chains of subgroups with given properties is another approach to classifying groups.

In order to get useful information about a group G, often it is enough to require that each subgroup in the chain is normal in its successor, rather than in the whole of G. In any case, the key idea is to make the chain as long as possible. This is achieved by requiring the quotient groups formed from successive subgroups to be, in some sense, as small as possible. A suitable sense of 'small' for these quotients is that they should have no non-trivial normal subgroup, because otherwise the chain can be extended using the Correspondence Theorem – you will see this in Exercise 4.2.

We first name groups that give rise to small quotients in this sense.

Definition 4.4 *Simple group*

A group G with more than one element is said to be a **simple group** if it has no non-trivial proper normal subgroups.

In the following exercise, you are asked to work with a chain of subgroups each of which is normal in its successor.

Exercise 4.2

Let G be a group with a chain of subgroups

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_s = G,$$

where H_i is a normal subgroup of H_{i+1} for $i \in \{0, \ldots, n-1\}$.

Suppose that K is a proper non-trivial normal subgroup of H_{i+1}/H_i. Show that the chain of subgroups can be extended to

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_i \subset J \subset H_{i+1} \subset \cdots \subset H_s = G,$$

where the inclusions are all proper (that is, $H_i \subsetneq H_{i+1}$).

The aim of the next exercise is to show that A_5 is a simple group.

Exercise 4.3

(a) Write down the cycle types of elements of A_5 together with the number of elements of each type.

(b) Use the list in part (a) to divide A_5 into conjugacy classes, remembering that some of the cycle types may split into more than one conjugacy class in A_5 if the conjugating elements in S_5 are odd permutations.

(c) Deduce that A_5 is a simple group.

We now give a description of a chain of subgroups that all finite groups possess.

Definition 4.5 *Composition series*

Let G be a group and suppose that $\{e\} = H_0, H_1, \ldots, H_n = G$ are subgroups of G such that:

(a) $\{e\} = H_0 \subset H_1 \subset \cdots \subset H_{n-1} \subset H_n = G$

(b) H_i is a normal subgroup of H_{i+1} for $i = 1, \ldots, n-1$

(c) H_{i+1}/H_i is a simple group for $i = 0, \ldots, n-1$.

Then we say that $H_0, H_1, \ldots, H_n$ are a **composition series** for G of **length** n.

Example 4.6 *Composition series for S_3 and S_4*

$\{e\} \subset A_3 \subset S_3$ is a composition series for S_3.

$\{e\} \subset \{e, (12)(34)\} \subset V \subset A_4 \subset S_4$ is a composition series for S_4, where V is the Klein group regarded as a subgroup of S_4, that is $V = \{e, (12)(34), (13)(24), (14)(23)\}$.

It is not hard to see that every finite group has a composition series: starting with the group G, identify a maximal normal subgroup N (and remember that such a subgroup always exists, because $\{e\}$ is normal in any group). Maximality ensures that the quotient group is simple. Continue in this way until $\{e\}$ is reached.

An important result that makes composition series a relevant tool for classification is the Jordan–Hölder Theorem. This says that any two composition series of the same group have the same length, and that the quotient groups in each series can be put into one–one correspondence with matching pairs being isomorphic.

For example, the dihedral group D_4 has two normal subgroups of order 4: the group of rotations $R = \langle r \rangle$ and the Klein group V. The subgroup $\{e, r^2\}$ is contained in both R and V, so D_4 has two composition series:

$$\{e\} \subset \langle r^2 \rangle \subset R \subset D_4 \quad \text{and}$$
$$\{e\} \subset \langle r^2 \rangle \subset V \subset D_4.$$

Although these two series are different, they have the same length and all the quotient groups are cyclic and of order 2, so they are isomorphic.

Since groups of prime order are cyclic and necessarily simple, groups where the quotient groups in the composition series have prime order are of particular interest.

Definition 4.7 *Soluble group*

Let G be a group and suppose that G has subgroups $\{e\} = H_0, H_1, \ldots, H_n = G$ such that

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_{n-1} \subset H_n = G,$$

where H_i is a normal subgroup of H_{i+1} and H_{i+1}/H_i is a cyclic group of prime order for $i = 0, \ldots, n-1$.

Then G is said to be a **soluble group**.

Thus, finite p-groups are soluble by Theorem 4.3. A key example of a group that is not soluble is S_5. This is because A_5 is simple, thus a composition series for S_5 is

$$\{e\} \subset A_5 \subset S_5,$$

and the quotient $A_5/\{e\}$ is simple but not of prime order.

There is a famous branch of mathematics, known as Galois Theory, that uses group theory to obtain results about the solvability of polynomial equations *by radicals*.

A *polynomial equation* of *degree* n is an equation of the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0, \quad a_n \neq 0$$

where the a_i are real numbers, or complex numbers, or elements of more general algebraic structures. You have met polynomial equations with real coefficients in your previous studies. For example, quadratic equations such as

$$4x^2 + 3x - 17 = 0$$

are polynomial equations of degree 2.

The phrase 'solving by radicals' means solving an equation through a process that combines standard arithmetic operations with taking successive roots. The familiar formula that says that the solutions of the quadratic equation

$$ax^2 + bx + c = 0, \text{ for } a \neq 0$$

are given by $\dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ is an example of a solution by radicals.

Galois Theory associates a subgroup of the symmetric group S_n to a polynomial equation of degree n. It turns out that the subgroup is soluble if, and only if, the equation can be solved by radicals. Unfortunately, here we do not have space to discuss any of the details of this association, but you will be in a good position to read further on the subject when you have completed this module.

Since S_2, S_3 and S_4 are all soluble groups, the association that we have just described can be used to show that polynomial equations of degree up to 4 can always be solved by radicals. Indeed, algorithms for such solutions were in existence long before Galois Theory was developed, although those for degree 3 and 4 came a long time after the formula to solve quadratic equations.

However, as S_5 is not soluble, and neither is S_n for $n > 5$, any polynomial equation whose associated group is the whole of S_5, or indeed S_n for $n > 5$, cannot be solved by radicals.

This is a very powerful result: it means that for polynomial equations of degree greater than or equal to 5, we cannot hope to find a general formula that will give us the solutions in terms of a finite number of additions, subtractions, multiplications, divisions and root extractions of the coefficients.

Learning outcomes

We list those topics on which we may set assessment questions to test your understanding of the chapter.

After working through this chapter you should be able to:

(a) Express products of elements of a group defined by generators and relations in an appropriate standard form.

(b) Recognise the dihedral and dicyclic groups when described using a standard form.

(c) Find subgroups generated by finite sets in simple cases.

(d) Find centres and centralisers of groups in simple cases.

(e) Find the class equation of groups of small order, including S_n.

(f) Apply the type of argument used to classify groups of order up to 14.

(g) Find the composition series of a group in simple cases.

(h) Construct proofs, similar to those in the chapter, based on the group axioms and the results of the chapter.

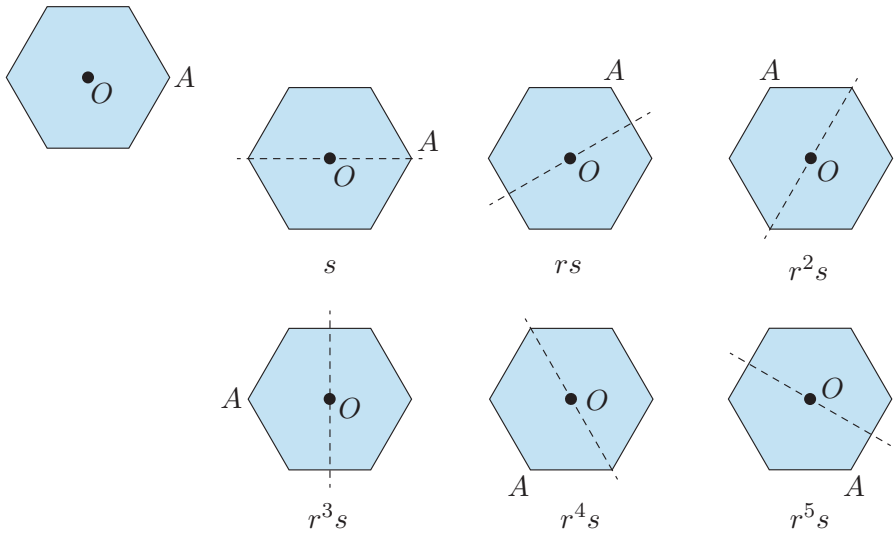
Solutions to exercises

Solution to Exercise 1.1

(a) All the rotations in D_6 are obtained by repeating r a sufficient number of times. Thus the rotations are

$$r,\ r^2,\ r^3,\ r^4,\ r^5,\ r^6 = r^0 = e.$$

(b) The easiest way to find out which reflection corresponds to each expression of the form $r^n s$ is to keep track of what happens to the vertices of the hexagon under each composite transformation. These transformations are illustrated in the figure below.



(c) By inspection, we find that $sr = r^5 s$.

You may have expressed this element in the form $r^{-1}s$, which is the same because $r^{-1} = r^5$.

Solution to Exercise 1.2

(a) $sr^2 = srr = r^5 sr = r^5 r^5 s = r^{10} s = r^4 s$

$sr^3 = sr^2 r = r^4 sr = r^4 r^5 s = r^9 s = r^3 s$

The second result should be no surprise as r^3 is rotation through π and so commutes with all the elements of D_6. If you spotted this and used it in your solution, well done!

(b) $s^5 = s$

Solution to Exercise 1.3

(a) This is the cyclic group $\mathbb{Z}_6$.

(b) This is the dihedral group D_4 – the symmetry group of a square.

(c) This is the Klein group $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

The relation $sr = rs$ means that the two generators commute. A little thought might convince you that this implies the group is abelian. In addition, the standard form shows the group has four elements, and it is not hard to see that no element has order greater than 2. These conditions are enough to show that the group is isomorphic to V.

Solution to Exercise 1.4

(a) Firstly we show that N is a subgroup of G.

Closure The only non-trivial product to check is $r^2r^2 = e$. So N satisfies the closure axiom.

Identity As e is in N, the identity axiom is satisfied.

Inverses As $e^{-1} = e$ and $\left(r^2\right)^{-1} = r^2$, the inverses axiom is satisfied.

Hence N is a subgroup of G.

Alternatively, simply note that $N = \langle r^2 \rangle$.

Next, we must show that N is normal. By Proposition 3.7 of Chapter 5, we need to check that aNa^{-1} is a subset of N for each a in G.

As $aea^{-1} = e \in N$ for each a in G, we only have to check that ar^2a^{-1} is in N. Using the relations $r^4 = s^2 = e$ and $sr = r^3s$ gives the following.

$$\begin{aligned}
er^2e^{-1} &= r^2 \\
rr^2r^{-1} &= r^2 \\
(r^2)r^2(r^2)^{-1} &= r^2 \\
(r^3)r^2(r^3)^{-1} &= r^2 \\
sr^2s^{-1} &= r^2 \\
(rs)r^2(rs)^{-1} &= r^2 \\
(r^2s)r^2(r^2s)^{-1} &= r^2 \\
(r^3s)r^2(r^3s)^{-1} &= r^2
\end{aligned}$$

This completes the proof that N is a normal subgroup of G.

(b) The distinct left cosets of $N = \{e, r^2\}$ are

$$\begin{aligned}
eN &= r^2N = N, \\
rN &= r^3N = \{r, r^3\}, \\
sN &= r^2sN = \{s, r^2s\}, \\
rsN &= r^3sN = \{rs, r^3s\}.
\end{aligned}$$

(c) The Cayley table of G/N is as follows.

$\circ$	N	rN	sN	rsN
N	N	rN	sN	rsN
rN	rN	N	rsN	sN
sN	sN	rsN	N	rN
rsN	rsN	sN	rN	N

Solution to Exercise 1.5

(a) $\overline{K}_1 = \{N, rsN\}$, $\overline{K}_2 = \{N, r^2sN\}$.

(b) $K_1 = \{e, r^3, rs, r^4s\}$, $K_2 = \{e, r^3, r^2s, r^5s\}$.

Solution to Exercise 1.6

(a) $b^4 = (b^2)^2 = a^4 = e$

(b) $b^2a = a^2a = a^3 = aa^2 = ab^2$ and $b^2b = b^3 = bb^2$

(c)
$$\begin{aligned} aba^3b = e &\Rightarrow aaba^3b = a \\ &\Rightarrow ba^2ba^3b = ba \\ &\Rightarrow b^4a^3b = ba && \text{using } a^2 = b^2 \\ &\Rightarrow a^3b = ba && \text{using } a^4 = e \text{ and } a^2 = b^2 \end{aligned}$$

(d) The result in part (c) means that in any word involving a and b we can successively move all the bs to the right. This will give us a word of the form $\alpha\beta$, where α is a word containing only as and β is a word containing only bs.

We can then use $a^4 = e$ and $b^4 = e$ to reduce α and β to a^r and b^s respectively for some $r, s \in \{0, 1, 2, 3\}$.

Lastly, we can use $b^2 = a^2$ and $b^3 = a^2b$ to write an element g of Dic_2 in the form $g = a^rb^s : \ r = 0, \ldots, 3, \ s = 0, 1$.

Solution to Exercise 1.7

(a) We have

$$a^2 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{and}$$

$$b^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix},$$

so $a^2 = b^2$. Moreover, $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, that is, $(a^2)^2 = a^4 = e$.

Another matrix calculation shows that $aba^3b = e$.

Calculation also shows that the eight matrices

$$a^rb^s : \ r = 0, \ldots, 3, \ s = 0, 1$$

are distinct, and the required result follows.

(b) Both $\langle a \rangle$ and $\langle b \rangle$ are cyclic subgroups of order 4. Moreover, the product $ab = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$ also generates a cyclic subgroup of order 4. Since $|G| = 8$, these three subgroups of order 4 have index 2 in G, and so they are normal.

Solution to Exercise 1.8

Since $a^4 = e$, we have $a^3 = a^{-1}$.

Since $a^2 = b^n$ and $a^4 = e$, we have $a^4 = (b^n)^2 = b^{2n} = e$, hence

$$b^{2n-1} = b^{-1}.$$

Now $aba^3b = e \Rightarrow ba^3b = a^{-1} = a^3$
$\Rightarrow ba^3 = a^3b^{-1} = a^3b^{2n-1}$
$\Rightarrow ba^3 = a^3a^2b^{n-1} = ab^{n-1}$
$\Rightarrow ba = ab^{n-1}a^2 = a^3b^{n-1}$.

We can use this relation to rewrite any word in a, b as a word in a followed by a word in b, that is, a power of a followed by a power of b. We then use

$$a^4 = e, \quad a^2 = b^n$$

to ensure that the power of a is one of $a^0(= e), a, a^2, a^3$ and the power of b is one of $b^0(= e), b, \ldots, b^{n-1}$.

This shows that every element of Dic_n can be written in the required form. Since this form gives $4n$ elements and Dic_n has order $4n$, we have a standard form.

Solution to Exercise 1.9

Let $H = \langle S \rangle$. Since $(1\,2\,3) = (1\,2)(2\,3)$, it is clear that $H \subseteq A_4$.

Now $a = (1\,2\,3)$ has order 3 and $b = (1\,2)(3\,4)$ has order 2, so H has order at least 6. Since $|A_4| = 12$, either $|H| = 6$ or $|H| = 12$. We have that

$$ab = (1\,2\,3)(1\,2)(3\,4) = (1\,3\,4),$$
$$a^2b = (1\,3\,2)(1\,2)(3\,4) = (2\,3\,4),$$
$$ba = (1\,2)(3\,4)(1\,2\,3) = (2\,4\,3).$$

It follows that $\{e, a, a^2, b, ab, a^2b, ba\} \subseteq H$, so H contains at least seven distinct elements of A_4. Therefore we must have $|H| = 12$, hence $H = A_4$ as required.

Solution to Exercise 1.10

We have $b^{-1} = b$, so

$$bab^{-1} = (2\,5)(3\,4)(1\,2\,3\,4\,5)(2\,5)(3\,4) = (1\,5\,4\,3\,2).$$

Since $(1\,5\,4\,3\,2) = a^{-1}$ and a has order 5, we can deduce

$$bab^{-1} = a^{-1} = a^4,$$

hence $ba = a^4b$. By Proposition 1.7 we know that

$$H = \{s_1^{r_1} \cdots s_n^{r_n} : n \in \mathbb{N}, s_i \in \{a, b\}, r_i \in \mathbb{Z}, i = 1, \ldots, n\}.$$

Since $ba = a^4b$ we can successively swap terms in any expression $s_1^{r_1} \cdots s_n^{r_n}$ so that the expression can be written as $a^r b^s$. Since $a^5 = b^2 = e$, we have that $H = \{a^r b^s : r = 0, \ldots, 4, s = 0, 1\}$. This set contains at most ten elements. Note that we have to say 'at most' since we cannot be sure that these elements are distinct.

The order of a is 5 and that of b is 2. Hence by Proposition 4.5 of Chapter 5, both 5 and 2 divide the order of H. Therefore $|H|$ is a multiple of 10, and hence at least 10.

Thus we have shown that the order of H is 10, as required.

Solution to Exercise 2.1

(a) $srs^{-1} = r^4$ and $rsr^{-1} = rsr^4 = r^2s$ in D_5.

(b) $srs^{-1} = r^5$ and $rsr^{-1} = rsr^5 = r^2s$ in D_6.

Solution to Exercise 2.2

To find a conjugacy class $\mathrm{Conj}_G(a)$, we compute the conjugates gag^{-1} and use some ingenuity to reduce the number of calculations. Proposition 2.5 is useful. In particular:

- a is conjugate to b if, and only if, $\mathrm{Conj}_G(a) = \mathrm{Conj}_G(b)$
- all the elements of a conjugacy class have the same order
- $|\mathrm{Conj}_G(a)|$ divides $|G|$ whenever G is a finite group.

(a) In D_4, the relation $sr = r^3s$ is equivalent to the more general relation $sr = r^{-1}s$, which holds in *any* dihedral group. From this we get $sr^{-1} = rs$, and repeatedly multiplying on the left by r and simplifying gives the useful relation

$$sr^{-i} = r^i s,$$

which holds in *any* dihedral group.

In D_4, taking $i = 2$ gives

$$sr^{-2} = sr^2 = r^2 s,$$

which means that r^2 commutes with s. Since r^2 also commutes with every element of the form r^i, it commutes with every element of D_4.

We therefore have two single-element conjugacy classes, $\{e\}$ and $\{r^2\}$.

Now consider the element r. First we try conjugating r by s (this makes the calculations easy). We get

$$srs^{-1} = r^{-1}ss^{-1} = r^{-1} = r^3,$$

so $r^3 \in \mathrm{Conj}(r)$. There are no other elements of order 4 in D_4, so $\{r, r^3\}$ is the whole of $\mathrm{Conj}(r)$.

Now consider the elements s and rs. First we try conjugating s by r and rs by r^{-1} (again to make the calculations easy). We get

$$rsr^{-1} = rrs = r^2 s$$

and

$$r^{-1}(rs)r = sr = r^3 s.$$

These elements form either two conjugacy classes, $\{s, r^2 s\}$ and $\{rs, r^3 s\}$, or a single one, $\{s, r^2 s, rs, r^3 s\}$. To determine which occurs, we calculate all the conjugates of s. Conjugating

- by an element of the form r^i (a rotation) gives $r^i s r^{-i} = r^i r^i s = r^{2i} s$
- by an element of the form $r^i s$ (a reflection) gives $r^i s s (r^i s)^{-1} = r^i s s r^i s = r^i r^i s = r^{2i} s$.

Thus, s is conjugate to $r^2 s$ but not to rs or $r^3 s$. The conjugacy classes are

$$\{e\}, \{r^2\}, \{r, r^3\}, \{s, r^2 s\} \text{ and } \{rs, r^3 s\}.$$

Therefore the class equation is $8 = 1 + 1 + 2 + 2 + 2$.

(b) By Exercise 1.8, in *any* dicyclic group Dic_n, we have

$$b^{-1} = b^{2n-1} = a^2 b^{n-1}$$

and

$$ba = a^3 b^{n-1} = ab^{-1}.$$

In Dic_2 these equalities become $b^{-1} = a^2 b$ and $ba = a^3 b = ab^{-1}$.

Now, $a^2 = b^2$, which means that a^2 commutes with b. Since a^2 also commutes with every element of the form a^i, it commutes with every element in Dic_2.

We therefore have two single-element conjugacy classes, $\{e\}$ and $\{a^2\}$.

To find the other conjugacy classes, we start by finding some specific conjugates. We try to choose conjugating elements that make the calculations as easy as possible.

First consider the element a: we have $bab^{-1} = a^3 bb^{-1} = a^3$, which gives $\{a, a^3\} \subseteq \mathrm{Conj}(a)$.

Now consider the element b: we have $a^{-1}ba = a^{-1}a^3 b = a^2 b$, which gives $\{b, a^2 b\} \subseteq \mathrm{Conj}(b)$.

Now consider the element ab: we have $b(ab)b^{-1} = ba = a^3 b$, which gives $\{ab, a^3 b\} \subseteq \mathrm{Conj}(ab)$.

Since the size of a conjugacy class divides the order of the group, these sets form either three disjoint conjugacy classes, or one conjugacy class of four elements and one of two. Unfortunately, we need some further calculation to determine which case occurs.

First we calculate all the conjugates of a:

$$a^i a a^{-i} = a \quad \text{and} \quad a^i ba(a^i b)^{-1} = a^i bab^{-1}a^{-i} = a^i a^3 a^{-i} = a^3,$$

so one conjugacy class is $\{a, a^3\}$.

Next we calculate all the conjugates of b (noting that a^{-i} is easier than a^i):

$$a^{-i}ba^i = a^{-i}a^3ba^{i-1} = \cdots = a^{-i}a^{3i}b = a^{2i}b$$

and

$$(a^ib)^{-1}b(a^ib) = b^{-1}(a^{-i}ba^i)b = b^{-1}(a^{2i}b)b = a^{2i}b^{-1}b^2 = a^{2i}b,$$

so another conjugacy class is $\{b, a^2b\}$. The final class is $\{ab, a^3b\}$.

The conjugacy classes are

$$\{e\}, \{a^2\}, \{a, a^3\}, \{ab, a^3b\}, \{b, a^2b\}.$$

Hence the class equation is $8 = 1 + 1 + 2 + 2 + 2$.

Solution to Exercise 2.3

(a) $\mathrm{Cent}_{S_3}(1\,2\,3) = \{e, (1\,2\,3), (1\,3\,2)\} = \langle(1\,2\,3)\rangle$, since $(1\,2)$ does not commute with $(1\,2\,3)$ and so the centraliser cannot be the whole group.

$\mathrm{Cent}_{S_3}(1\,2) = \{e, (1\,2)\} = \langle(1\,2)\rangle$, since $(1\,2\,3)$ does not commute with $(1\,2)$, and so the centraliser cannot be the whole group.

(b) $\mathrm{Cent}_{D_4}(r^2) = D_4$, since r^2 commutes with all the elements of D_4. So $\langle r^2\rangle \neq \mathrm{Cent}_{D_4}(r^2)$.

Since s and e commute with s, and so does r^2 (which in fact commutes with every element of D_4), we must have $\{e, s, r^2\} \subseteq \mathrm{Cent}_{D_4}(s)$. Since $\mathrm{Cent}_{D_4}(s)$ is a subgroup of D_4, we must have $r^2s \in \mathrm{Cent}_{D_4}(s)$. Moreover, r does not commute with s, so this centraliser cannot be the whole group. Therefore $\mathrm{Cent}_{D_4}(s) = \{e, s, r^2, r^2s\}$ and $\mathrm{Cent}_{D_4}(s) \neq \langle s\rangle$.

Solution to Exercise 2.4

(a) The centraliser of any element is the whole group.

(b) In any group G, we have $\mathrm{Cent}_G(e_G) = G$.

Solution to Exercise 2.5

Since H is a subgroup of $Z(G)$, it is also a subgroup of G and so we only need to show that H is normal in G.

As in the proof of Proposition 2.9, let $a \in H$ and $g \in G$. Then, since a is a central element of G, we have $gag^{-1} = a \in H$, so that H is a normal subgroup of G by Proposition 3.7 of Chapter 5.

Solution to Exercise 2.6

(a) $\mathrm{Cent}_{S_3}(1\,3) = \{e, (1\,3)\}$

(b) An element of the centre commutes with every other element, so in particular with $(1\,3)$. This gives $Z(S_3) \subseteq \mathrm{Cent}_{S_3}(1\,3)$. We know that $(1\,3)$ is not in the centre, for otherwise $\mathrm{Cent}_{S_3}(1\,3)$ would be the whole of S_3, so we have $Z(S_3) = \{e\}$.

Solution to Exercise 2.7

(a) $Z(\mathrm{Dic}_2) = \{e, a^2\}$.

(b) $\mathrm{Conj}_{\mathrm{Dic}_2}(a) = \{a, a^3\}$.

(c) The elements a^i all commute with a, so $\{e, a, a^2, a^3\} \subseteq \mathrm{Cent}_{\mathrm{Dic}_2}(a)$.

By Theorem 2.11,

$$|\mathrm{Cent}_{\mathrm{Dic}_2}(a)| = |G|/|\mathrm{Conj}_{\mathrm{Dic}_2}(a)| = \tfrac{8}{4} = 4.$$

Hence $\mathrm{Cent}_{\mathrm{Dic}_2}(a) = \{e, a, a^2, a^3\}$.

Solution to Exercise 3.1

Since a has order n, we have $|\langle a\rangle| = n$. Therefore $b \notin \langle a\rangle$, as the order of b is 2 and 2 does not divide n. Now $\langle b\rangle = \{e, b\}$, and so $\langle a\rangle \cap \langle b\rangle = \{e\}$. Therefore, by Lemma 2.7 of Chapter 6, the order of ab is $\mathrm{lcm}(2, n) = 2n$, as required.

Solution to Exercise 3.2

Recall that

$$D_6 = \{r^m s^n : m = 0, \ldots, 5, n = 0, 1; r^6 = s^2 = e, sr = r^5 s\}.$$

Let H be the subgroup of D_6 generated by r^2 and s, and let K be the subgroup generated by r^3. Then

$$H = \{e, r^2, r^4, s, r^2 s, r^4 s\} \quad \text{and} \quad K = \{e, r^3\},$$

so $H \cong D_3$ and $K \cong \mathbb{Z}_2$.

Moreover, H and K are both normal in D_6: H because it has index 2, and K because r^3 is central. Now every element of D_6 can be written in the form kh with $k \in K$ and $h \in H$, and $K \cap H = \{e\}$. Thus, by Proposition 1.9 of Chapter 6,

$$D_6 \cong K \times H \cong H \times K,$$

therefore $D_6 \cong D_3 \times \mathbb{Z}_2$, as required.

Solution to Exercise 3.3

From Exercise 5.5 of Chapter 5, we know that S_4 has five conjugacy classes, namely:

- $\{e\}$, of size 1
- the set containing the 4-cycles, of size 6
- the set containing products of 2-cycles, of size 3
- the set containing the 3-cycles, of size 8
- the set containing the 2-cycles, of size 6.

Since a subgroup of S_4 of size 12 is necessarily normal, it must be a union of conjugacy classes by Proposition 3.12 of Chapter 5. Moreover, any subgroup contains the identity, hence the conjugacy class of size 1. Therefore any subgroup of order 12 must contain the three pairs of 2-cycles, otherwise the order of the subgroup would be an odd number.

Then the only way to obtain 12 elements as a union of conjugacy classes is to include the eight 3-cycles. This gives A_4, as required.

Solution to Exercise 3.4

We know that

$$\mathrm{Dic}_3 = \{a^r b^s : r = 0, \ldots, 3,\ s = 0, \ldots, 2; a^4 = e, a^2 = b^3, aba^3b = e\},$$

and $ba = a^3b^2 = ab^{-1}$ (see Exercise 1.8).

Then:

- b and $b^5 = a^2b^2$ have order 6
- b^2 and $b^4 = a^2b$ have order 3
- $a^2 = b^3$ has order 2
- $a, a^3, ab, a^3b, ab^2, a^3b^2$ all have order 4.

To see that ab, a^3b, ab^2 and a^3b^2 all have order 4, note that ab and a^3b are inverse to each other, and so they have the same order. To check that their order is 4, note that

$$abab = a(ab^{-1})b = a^2.$$

Likewise, ab^2 and a^3b^2 are inverse to each other and

$$ab^2ab^2 = abab^{-1}b^2 = abab\,,$$

so these two elements also have order 4.

Solution to Exercise 3.5

Since b has order 6, we have that b and $b^5 = b^{-1}$ are the two elements of order 6 and that b^2 and b^4 are the two elements of order 3.

Since a has order 4, a^2 has order 2. Similarly, b^3 has order 2. Since G has a unique element of order 2, we have that $a^2 = b^3$.

The element ab cannot be the unique element of order 2, otherwise $ab = a^2$, which implies $b = a$, contradicting the fact that a and b have different orders. The element ab cannot have order 3, because otherwise either $ab = b^2$ or $ab = b^4$, either of which gives a contradiction, as above.

Finally, the element ab cannot have order 6, because otherwise either $ab = b$ or $ab = b^5$, either of which gives a contradiction. The only remaining possibility is that ab has order 4. This means that $(ab)^2$ has order 2 and hence that $(ab)^2 = a^2$.

Now, $abab = a^2$ implies that $bab = a$ and hence that

$$ba = ab^{-1} = ab^5 = a^3b^2.$$

Finally, $aba^3b = ab(a^3b^2)b^{-1} = abbab^{-1} = ab^2ba = ab^3a = aa^2a = a^4 = e$.

Hence G satisfies all the relations $a^4 = e$, $a^2 = b^3$ and $aba^3b = e$, and therefore G is Dic_3.

Solution to Exercise 4.1

If $Z(G)$ has order p^2, then the quotient group $G/Z(G)$ has order p and is therefore cyclic. Then, by Theorem 2.14, G is abelian, which implies that $Z(G) = G$ has order p^3, a contradiction. Thus $Z(G)$ cannot have order p^2.

Solution to Exercise 4.2

Since K is a proper non-trivial normal subgroup of H_{i+1}/H_i, by the Correspondence Theorem there is a proper normal subgroup J of H_{i+1} that properly contains H_i. The chain can therefore be extended to

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_i \subset J \subset H_{i+1} \subset \cdots \subset H_s = G.$$

Solution to Exercise 4.3

(a)

Cycle type	Number of elements
(1)(2)(3)(4)(5)	1
(--)(--)	15
(---)	20
(-----)	24

(b)

Representative of conjugacy class	Size of conjugacy class
(1)(2)(3)(4)(5)	1
(1 2)(3 4)	15
(1 2 3)	20
(1 2 3 4 5)	12
(1 3 5 2 4)	12

(c) By Proposition 3.12 of Chapter 5, we know that any normal subgroup of A_5 is a union of conjugacy classes, so that any non-trivial normal subgroup must contain $\{e\}$ and at least one other conjugacy class. We also know that the order of a subgroup must divide $|A_5| = 60$.

Since it is impossible to find a union of conjugacy classes of A_5 that includes the identity and at least one other class that is not the whole group, and whose size divides 60, we conclude that A_5 has no proper non-trivial normal subgroups and is therefore a simple group.